HOCHSCHULE MITTWEIDA
UNIVERSITY OF APPLIED SCIENCES

Masterarbeit

Frau M.A.
Hanna Sintermann

Integration von Governance, Risikomanagement und Compliance Management in das Geschäftsprozessmanagement

München, 2015

Institut für Technologie- und Wissenstransfer
Mittweida (ITWM)

Masterarbeit

Integration von Governance, Risikomanagement und Compliance Management in das Geschäftsprozessmanagement

Autor:
Frau M.A.

Hanna Sintermann

Studiengang:
Master Prozess- und Projektmanagement

Erstprüfer:
Erich Dräger

Zweitprüfer:
Prof. Dr. Steffen Rößler

Einreichung:
München, 15. Dezember 2015

Verteidigung/Bewertung:
München, 2016

Insitute for technology and knowledge transfer
Mittweida (ITWM)

MASTERTHESIS

Integration of Governance, Risk Management , and Compliance Management into Business Process Management

author:
Ms. M.A.

Hanna Sintermann

course of studies:
master project- and processmanagement

first examiner:
Erich Dräger

second examiner:
Prof. Dr. Steffen Rößler

submission:
Munich,15. December 2015

defence/ evaluation:
Munich, 2016

Bibliografische Beschreibung:

Sintermann, Hanna:
Integration von Governance, Risikomanagement und Compliance Management in das Geschäftsprozessmanagement. - 2015. - VI, 64, 2 S.
Mittweida, Hochschule Mittweida, Institut für Technologie- und Wissenstransfer Mittweida (ITWM), Masterarbeit, 2015

Referat:

Durch Globalisierung, den immer schneller voranschreitenden Produktinnovationen und Käufermärkten sind Unternehmen mit einer hohen Marktdynamik konfrontiert. Zudem sind die GRC-Disziplinen gegenwärtig von großer Bedeutung für eine Vielzahl von Unternehmen. Eine kontinuierlich wachsende Zahl von Gesetzen, Regularien und Standards zwingt die Mehrheit der Unternehmen sich verstärkt mit diesen Anforderungen auseinanderzusetzen. GRC-Management in die Geschäftsprozessen zu integrieren, kann zur Erreichung der Unternehmensziele und dem nachhaltigen Unternehmenserfolg beitragen.

Die vorliegende Arbeit befasst sich mit der Integration von GRC-Management in das Geschäftsprozessmanagement. Das Hauptziel besteht darin, ein Vorgehensmodell zur integrierten Implementierung von Prozessen mit den GRC-Disziplinen zu entwerfen, um damit aktuelle Anwendungsdefizite im Vorgehen zur Einführung von GRC- und Geschäftsprozessmanagement zu adressieren und Unternehmen zu einem Wettbewerbsvorteil zu verhelfen. Dazu werden die Grundlagen des GRC- und des Prozessmanagement analysiert und aus ausgewählten Vorgehensmodellen zur Einführung von GPM und GRC-Management Kenntnisse für das zu erstellende integrierte Vorgehensmodell im Bereich des Geschäftsprozessmanagement abgleitet.

Inhalt

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

BPM	Business Process Management
BPR	Business Process Redesign
CEO	Chief Executive Officer
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CMS	Compliance-Management-System
CPO	Chief Process Officer
DCGK	Deutscher Corporate Governance Kodex
GPM	Geschäftsprozessmanagement
GRC	Governance, Risiko und Compliance
IDW	Institut der Wirtschaftsprüfer
IT	Informationstechnologie
KVP	Kontinuierlicher Verbesserungsprozess
PKR	Prozesskostenrechnung
PM	Prozessmanagement
PS	Prüfungsstandard
PV	Prozessverantwortliche(r)
RM	Risikomanagement
TQM	Total Quality Management

1 Motivation, Zielsetzung und Aufbau

Durch scheinbar endlose wirtschaftskriminelle Skandale, Bilanzskandale und Organisationen die nicht kalkulierte und infolge ruinöse Risiken eingehen, sind die eng zusammenhängenden Themen Governance, Risikomanagement und Compliance (GRC) zu unausweichlichen Themen in der Wirtschaftswelt geworden. Jede Organisation muss Ressourcen in diese Themen investieren. "Hauptursache für die meisten Unternehmenskrisen waren damals wie heute Fehler des Managements, das im Auftrag der Eigentümer die Geschäfte der Gesellschaft führt und ihr Vermögen verwaltet" (Menzies, 2009, S. 4). Mit Hilfe der effektiven Implementierung der GRC-Disziplinen im Unternehmen, versucht man diesen Management-Fehlern proaktiv zu begegnen.

"Dass Unternehmen und durch sie Beauftragte sich bei ihrer wirtschaftlichen Tätigkeit an rechtliche, professionelle und gesellschaftliche Regeln halten müssen, ist die ordnungspolitische Grundlage der Marktwirtschaft" (Wieland et. al, 2010, S.5). Es gibt aber auch diverse gesetzliche Bestimmungen und Leitlinien (z.B. der Deutsche Corporate Governance Codex), die Organisationen genau dazu verpflichten.

Die Vernachlässigung dieser Themen kann "für Unternehmen zu gravierenden ökonomischen Konsequenzen führen" (Marekfia und Nissen, 2009, S.2). Darüber hinaus können die Konsequenzen für Unternehmen auch rechtlicher Natur sein, wie "Haftstrafen und Entlassungen für straffällige Mitarbeiter, aber auch Unternehmensleitung und Organe, Geldbußen/ Geldstrafen, Gewinnabschöpfung etc., sowie ein Risiko für die Reputation des Unternehmen – wobei die Dimensionen interdependent sind, d.h. die rechtlichen Risiken können sich u. U. auch finanziell auswirken, ebenso wie sich auch Reputationsschäden in einem Verlust von Kunden oder Investoren zeigen können" (Schweikert, 2014, S. 29).

Das sinnvolle Einsetzen und Umsetzen der GRC Themen im Unternehmen kann nicht nur finanzielle, rechtliche und Reputationsschäden verhindern, sondern auch ökonomische Vorteile schaffen. Die Aktivitäten in Governance, Risiko und Compliance sind eng miteinander verwoben. Sie greifen auf die gleichen Prozessen, Mitarbeiter und Informationen zurück. Berücksichtigt man diese Synergiepotenziale und führt diese Themen strukturiert und strategisch ein, so können fundierte Entscheidungen getroffen werden und Risiken effizienter gesteuert werden.

Zusätzliche zu den Herausforderungen der GRC Aktivitäten, sind die Unternehmen mit einer hohen Marktdynamik konfrontiert. Es herrscht ein Käufermarkt vor. Es gibt ein Überangebot an Produkten und Dienstleistungen. Dadurch und durch die immer weiter voranschreitende Globalisierung müssen Unternehmen sehr schnell auf den Markt und auf wechselnde Kundenbedürfnisse reagieren können und die Fähigkeit haben, qualitativ

hochwertige Produkte in kurzer Zeit zu liefern, um Konkurrenzfähig zu bleiben (Dräger und Rößler, 2012).

Daraus ergibt sich für Unternehmen, die erfolgreich bleiben wollen ,dass sie zum Einen ihre Geschäftsrisiken (inklusive der regulatorischen Risiken) genau kennen und im Auge behalten müssen, aber auch den Vorteil einer konsequenten Prozessorientierung nutzen sollten. Mit Hilfe des Prozessmanagement können sich Organisationen flexibel auf Kundenbedürfnisse ausrichten, die Durchlaufzeiten optimieren und die Motivation und Identifizierung der Mitarbeiter mit Ihrer Aufgabe und dem Unternehmen maximieren. "Die Unternehmen müssen heutzutage mehr denn je in der Lage sein, integrierte Geschäftsprozesse zu schaffen und diese flexibel an die laufenden Veränderungen anpassen." (PwC, 2011)

1.1 Problemstellung und Motivation

Sowohl GRC Aktivitäten als auch die Geschäftsprozesse einer Organisation orientieren sich an deren Strategie und den übergeordneten Zielen. Geschäftsprozesse müssen verschiedene Arten von Compliance-Anforderungen einhalten. Die Implementierung von neuen Geschäftsprozessen oder die Veränderung von bestehenden beeinflussen die Bewertung von assoziierten Risiken und das wiederum kann zu neuen Regelungen im Unternehmen führen. Zusätzlich können durch die Überwachung und Analyse von Prozessen auch die darin enthaltenen Regelungen überprüft werden und das Ergebnis wiederum Einfluss auf das Compliance Management haben.

Die Themen Governance, Risiko und Compliance sind eng verwoben mit den Geschäftsprozessen eines Unternehmens. Die Aktivitäten im Prozessmanagement und in den GRC Bereichen beeinflussen sich gegenseitig.

Trotzdem werden diese Themen häufig isoliert voneinander betrachtet und getrennt eingeführt. Ein proaktives und strategisches Vorgehen ist häufig nicht die Tatsache in heutigen Unternehmen. Laut Marekfia und Nissen (2009, S.3) wird im GRC-Management häufig Einzelfall-bezogen und reaktiv gehandelt: "Bestehende Abhängigkeiten werden nicht berücksichtigt, was die Nutzung von Synergiepotentialen verhindert. Der Bereich GRC wird außerdem überwiegend als 'Kostenverursacher' wahrgenommen." Weiter wird postuliert, dass durch diese nicht integrative Vorgehensweise mögliche Nutzeneffekte nicht erzielt werden können.

Ein möglicher und sehr effektiver Nutzen wäre die Optimierung der Geschäftsprozesse im Unternehmen. Was dazu führen würde, das GRC-Management nicht nur Kosten verursacht, sondern im Gegenteil auch an anderer Stelle Kosten minimiert und den Gewinn steigert. So berichten Sadiq, Governatore und Naimiri (2007), dass in einer Studie bis zu 80% der befragten Unternehmen einen wirtschaftlichen Nutzen von der Verbesserung ihrer Compliance-Systeme erwarten.

Wissenschaft und Gesellschaft konzentrieren sich häufig nur auf einzelne Problemstellungen und Themen und beschäftigen sich mit diesen meist nur getrennt voneinander. So sind z.B. diverse ISO-Normen in Unternehmen weit verbreitet, die verschiedene Gebiete, wie Qualitätsmanagement, Risikomanagement und Compliance-Management isoliert voneinander betrachten (Schnetzer, 2014).

Auch eine Compliance-Studie, durchgeführt von NTT DATA (2013), kommt zu dem Ergebnis, dass in vielen Unternehmen die GRC Themen nicht integriert werden und der strukturelle Rahmen unzureichend ist. Laut dieser Studie verfügen 23 Prozent der befragten Unternehmen nicht über eine formelle und strukturierte Compliance Organisation und eine "Zusammenarbeit mit dem Risikomanagement und dem Internen Kontrollsystem findet sich nur in einem Viertel der Unternehmen. Dadurch werden Risiken nicht ganzheitlich betrachtet und Effizienzpotentiale bleiben ungenutzt" (NTT DATA, 2013).

Diese derzeitigen Defizite beim Umgang mit GRC und Prozessmanagement und die großen Vorteile einer integrativen Gestaltung sind ein wesentlicher Motivationsfaktor dieser Arbeit. Auch Marekfia und Nissen (2009, S.3) haben festgestellt: "Bestehende Forschungsarbeiten in diesem Kontext diskutieren häufig ebenfalls Einzelfragen. Hierbei bleibt bislang unbeantwortet, wie die vereinzelten Vorschläge und Methoden in einem umfassenden organisatorischen Ansatz zu integrieren sind."

Auch aus Sicht des Prozessmanagements sollte dieses mit anderen Managementdisziplinen wie dem GRC-Management verknüpft werden. So stellen Bayer und Kühn (2013, S. VII) fest, "dass derzeit Prozessmanagement sowie andere Managementansätze oftmals isoliert voneinander betrachtet und eingesetzt werden. Diese müssen aus unserer Sicht allerdings im Sinne eines integrierten Managementsystems im Zusammenhang genutzt werden." Von Kochanowski et. al (2014) wird weitergehend dazu festgestellt: "Die Synergien beim strategischen und operativen Prozessmanagement und den GRC-Themen können nur gehoben werden, wenn beides gemeinsam abgedeckt wird. Dann kann ein Mehrwert entstehen, der über die reine Erfüllung von Auflagen hinausgeht und eine effiziente, risikoarme und nachhaltige Geschäftsprozessbearbeitung sicherstellt."

Die Autorin schlussfolgert daher, dass große Vorteile daraus entstehen können, bei der Einführung eines GRC-Managements und des Prozessmanagements in einer Organisation strategisch und integrativ vorzugehen.

1.2 Zielsetzung und Forschungsfragen

Ziel dieser Arbeit ist es ein Vorgehensmodell zu skizzieren, mit dem Governance, Risikomanagement und Compliance Management bei der Einführung von Geschäftsprozessmanagement sinnvoll integriert werden können.

Dazu soll erst ein Überblick über die Einzel-Themen auf Basis der aktuellen Literatur gegeben werden, um eine Ausgangsbasis für eben diese Integration herzustellen.

Damit soll primär die nachfolgende übergeordnete Forschungsfrage im Verlauf der Arbeit geklärt werden:

- Wie können Governance, Risikomanagement und Compliance Management effektiv in das Geschäftsprozessmanagement integriert werden?

Darauf aufbauend sollen nachfolgende Fragestellungen, die zur Beantwortung der Forschungsfrage notwendig sind, ebenfalls geklärt werden:

- Welche Berührungspunkte bestehen bei GRC und Geschäftsprozessmanagement?
- Welchen Lösungsbeitrag kann die Integration zur Überwindung aktueller Herausforderungen in GPM und GRC hervorbringen?
- Welche Grenzen und Schwierigkeiten sind bei der Integration zu erwarten?
- Welche Voraussetzungen müssen für die Integration gegeben sein?

1.3 Aufbau der Arbeit

In Kapitel 2 wird der Hintergrund Prozessmanagement dargestellt und der Begriff Prozessmanagement definiert.

In Kapitel 3 werden zunächst die Begriffe Governance, Risiko und Risiko-Management sowie das Compliance-Management erläutert und der Begriff des strategischen, integrierten GRC-Managements erläutert.

Anschließend wird in Kapitel 4.1 ein Einführungsmodell für das Geschäftsprozessmanagement vorgestellt, das NOVACESS-Modell. In Kapitel 4.2. wird das Vorgehen bei der isolierten Einführung des GRC-Managements erläutert. Diese beiden Ansätze werden dann in Kapitel 4.3 kombiniert und es wird ein neues Einführungsmodell für die integrierte Implementierung von GRC-Management und Geschäftsprozessmanagement (GRC-GPM) entwickelt und skizziert.

Zur Reflexion der Arbeitsergebnisse wurden qualitative Interviews geführt sowie empirische Studien und Beispiele in der wissenschaftlichen Literatur herangezogen. Damit wurden der mögliche Beitrag des Models zur Überwindung aktueller Schwierigkeiten in GRC und GPM ermittelt (Kapitel 5) sowie Grenzen, Schwierigkeiten und Voraussetzungen beim Einsatz eines integrierten Vorgehens bei der Einführung von GRC-GPM untersucht (Kapitel 6).

Abschließend wird ein Fazit gezogen und ein kurzer Ausblick auf weiteren Forschungsbedarf gegeben. In *Abbildung 1: Aufbau der Arbeit* ist ein Überblick über die Inhalte und den Aufbau der vorliegenden Arbeit visualisiert.

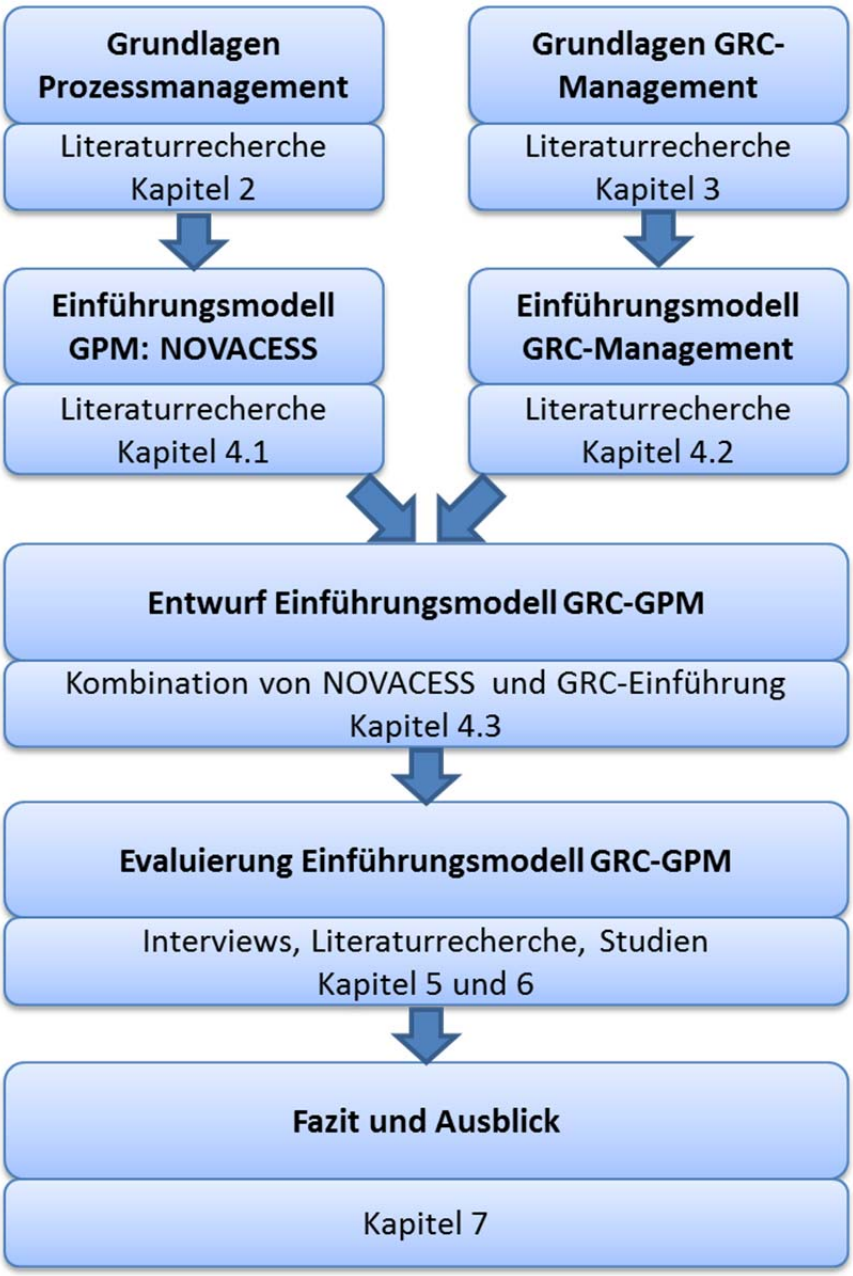


Abbildung 1: Aufbau der Arbeit

2 Grundlagen Prozessmanagement

Prozessmanagement ist inzwischen ein allgegenwärtiges Thema. Es wird von vielen Unternehmen als wesentliche Strategie angesehen, um Wettbewerbsvorteile zu erzielen, indem Geschäftsprozesse optimiert und überwacht werden. Die Beschreibung und Optimierung von Prozessen hilft auch funktionalen Organisationen die Arbeit an Schnittstellen zwischen Abteilungen zu verbessern. Eine Studie von PwC (2011) stellte fest, dass GPM bei den befragten Organisationen, unabhängig von deren Größe und Branche, ein sehr wichtiges Thema zur Organisationsentwicklung ist. "Die Mehrzahl sieht einen direkten Zusammenhangzwischen ihren Aktivitäten im Geschäftsprozessmanagement und ihrem heutigen Unternehmenserfolg." (PwC, 2011, S. 10)

Schon in der ersten Hälfte des letzten Jahrhunderts kam erstmalig der Gedanke des Prozessmanagements auf. Fritz Nordsiek erkannte bereits 1934 die Notwendigkeit der Prozessorientierung. Durch den 2. Weltkrieg unterbrochen, beschäftigte man sich dann aber erst wieder ab den fünfziger Jahren mit dem Thema (Junker, 2014).

Erste vertiefende wissenschaftliche Arbeiten wurden aber erst in den 1980er Jahren unter anderem von Michael Gaitanides, Michael Porter und August-Wilhelm Scheer veröffentlicht (Becker, Kugeler und Rosemann, 2012). Nachdem sich in den 1990er Jahren die Mehrheit der Projekte zur Neuausrichtung von Betriebsabläufen ausschließlich um Geschäftsprozesse drehten, wird das Prozessmanagement neuerdings mit dem Ansatz der Kontinuierlichen Verbesserung in Einklang gebracht. Dieser Ansatz geht zurück auf die Total Quality Management Initiativen der 1980er Jahre und der Anstrengungen zu kontinuierlichen Verbesserungen, die aus der Arbeit von W. Edwards Deming in den 1950er Jahren entstanden sind (zur Muehlen und Ho, 2006).

Das Geschäftsprozessmanagement besteht aus der Identifizierung von Prozessen und der Modellierung, Implementierung, Ausführung, Überwachung und Auswertung dieser. Viele Organisationen konzentrieren sich immer noch sehr auf ihren funktionalen Aufbau, die Abteilungen und Bereiche und deren Hierarchie. Sie haben den Übergang zu einer prozessorinerten Organisation noch nicht bewältigt. Daher ist die Strukturierung eines Unternehmens rund um seine Geschäftsprozesse ein sehr populäres Thema in der Management- und auch der IT-Literatur (zur Muehlen und Ho, 2006).

2.1 Definitionen

2.1.1 Prozesse

Die generelle Bedeutung des Wortes *Prozess* wird wohl von jedem Verstanden, aber es existieren trotzdem fast so viele Definitionen dafür, wie Autoren die über dieses Thema schreiben. Ganz allgemein wird in einem Prozess ein Input über verschiedene Aktivitäten in ein Ergebnis umgewandelt und dazu werden bestimmte Ressourcen benötigt.

Dillerup und Stoi (2011, S. 484) definieren einen **Prozess** aus betriebswirtschaftlicher Sicht als „eine Folge logisch zusammenhängender Aktivitäten zur Erstellung einer kundenbezogenen Leistung“. Diese Leistung können Produkte oder Dienstleistungen sein, es gibt aber auch Definitionen, die den Geschäftsprozess beschreiben "als eine Menge von Aktivitäten, die gemeinsam ein Ziel verfolgen und typischerweise im Kontext von Organisationseinheiten mit definierten Rollen und Beziehungen ausgeführt werden" (Weilkens, Weiss und Grass, 2010, S. 42).

Ein **Geschäftsprozess** ist ein wesentlicher und direkt wertschöpfender Prozess, der immer vom Kunden zum Kunden verläuft. Er ist ein "spezieller Prozess, der der Erfüllung der obersten Ziele der Unternehmung (Geschäftsziele) dient und das zentrale Geschäftsfeld beschreibt" (Becker, Kugeler und Rosemann, 2012, S.7).

Alle im Unternehmen ablaufenden Prozesse bilden eine Prozessstruktur. Diese lassen sich in einem unterschiedlichen Detaillierungsgrad betrachten und bilden damit eine Prozesshierarchie (Dillerup und Stoi, 2011).

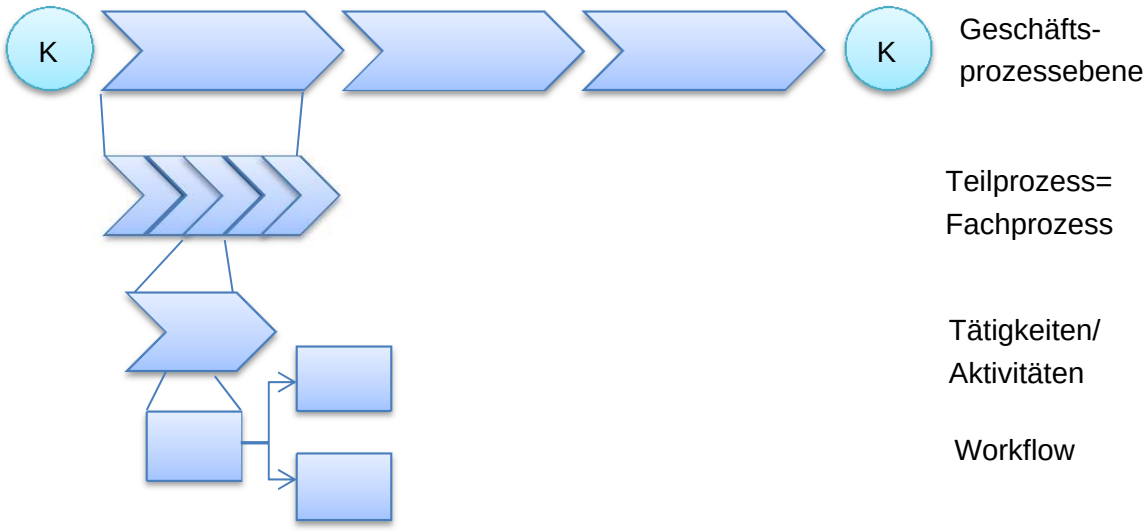


Abbildung 2: Struktur eines Geschäftsprozess

Abhängig davon wo die Prozesse in der Versorgungskette des Unternehmens angesiedelt sind, kann man (Kern-)Geschäftsprozesse und Unterstützungsprozesse unterscheiden.

Die erste Ebene der Prozesshierarchie bilden immer die **(Kern-)Geschäftsprozesse**. Diese richten sich direkt am Kundennutzen aus, gehen also vom Kunden zum Kunden (siehe Abbildung 1, K=Kunde). Die Geschäftsprozesse müssen sich nicht auf die Grenzen der Organisation beschränken, sondern können auch Aktivitäten bei Kunden, Lieferanten oder Partnern mit einschließen (Schmelzer und Sesselmann, 2013).

Unterstützende Tätigkeiten, die nicht direkt Teil eines Geschäftsprozesses sind, werden als **Unterstützungsprozesse** beschrieben. Dies ist ein "Prozess, dessen Aktivitäten aus Kundensicht zwar nicht wertschöpfend, jedoch notwendig sind, um einen Kernprozess ausführen zu können" (Becker, Kugeler und Rosemann, 2012, S.7).

Die Autoren zur Muehlen und Ho (2006) beschreiben die Komponenten und Eigenschaften eines Prozesses, die diesem zugeordnet sind. Dies sind zum einen seine Struktur, also z.B. der Kontrollfluss unter den einzelnen Aktivitäten, die Datenflussabläufe und die Regelungen, die Beschränkungen in der Prozessausführung beinhalten. Zum anderen sind dies seine Ziele und ergänzende Elemente wie z.B. Ressourcen, Input und Output.

2.1.2 Prozessverantwortliche

Damit Prozesse funktionieren und effizient gehalten werden, werden Prozessverantwortliche eingesetzt. Diese sind für den Prozessablauf und das Prozessergebnis verantwortlich, sowie für die funktionsübergreifende Planung, Steuerung und Kontrolle des Prozesses (Dillerup und Stoi, 2011).

2.1.3 Prozesslandkarte

In einer Prozesslandkarte können Prozesse einer Organisation übersichtlich eingeordnet werden (siehe Abbildung 3). Einzelne Geschäftsprozesse werden in ihren Wechselwirkungen untereinander grafisch dargestellt und es werden ggf. die Prozessverantwortlichen (siehe 2.1.2) definiert. Die Prozesslandkarte kann dann Grundlage für Optimierungen, Beschreibungen und Definitionen einer Prozessorganisation sein.

Prozesse zur Führung der Organisation werden als **Führungsprozesse**/ Managementprozesse bezeichnet.

Alle Aktivitäten, die zum operativen Tagesgeschäft gehören, fallen in den Bereich der Geschäftsprozesse und diejenigen, die von der Verwaltung zu erledigen sind und die Geschäftsprozesse unterstützten, sind in der Prozesslandkarte als Unterstützungsprozesse abgebildet (siehe 2.1.1). Ob man Prozesse wie Einkauf, Marketing, Logistik oder Vertrieb eher bei den Kerngeschäftsprozessen oder bei den Unterstützungsprozessen abbildet, hängt von der Bedeutung dieser Prozesse bei der Wertschöpfung in der einzelnen Organisation ab und muss im Einzelfall davon abhängig entschieden werden.

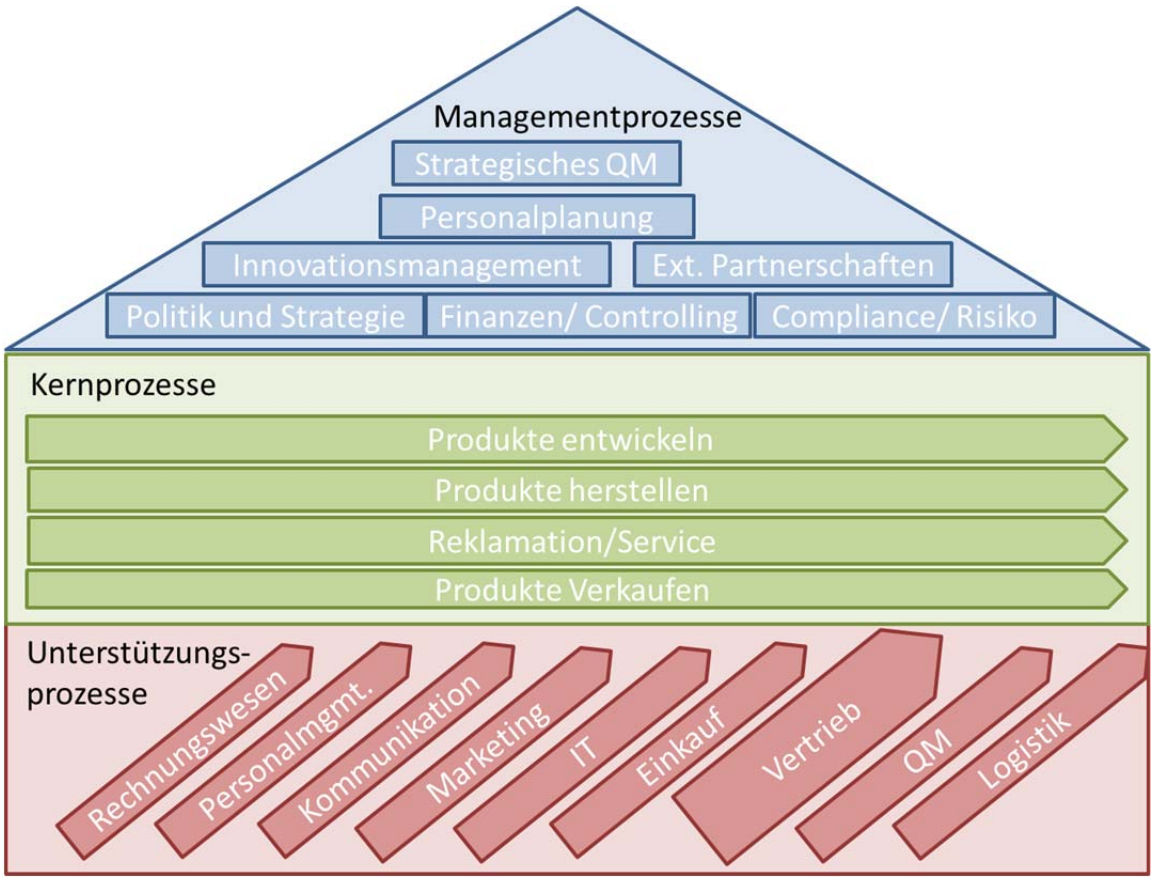


Abbildung 3: Beispiel Prozesslandkarte

2.1.4 Prozessmanagement

Die Gestaltung und die Organisation eines Unternehmens in Orientierung an Prozessen werden häufig als **Prozessmanagement** bezeichnet. Die internationale Bezeichnung ist **Business Process Management (BPM).** In dieser Arbeit wird der deutsche Begriff Geschäftsprozessmanagement (GPM) verwendet.

Weilkiens, Weiss und Grass (2010, S. 60) geben eine allgemeine und verbreitete Definition von Benner und Tuschmann wieder:

> Das Geschäftsprozessmanagement beinhaltet koordinierte Aufgaben, um die Prozesse der Organisation zu erfassen, zu verbessern und zu integrieren. In diesem Kontext wird die Organisation als ein System vernetzter Prozesse betrachtet.

In Anlehnung an Gaitanides etl al. definieren Dillerup und Stoi (2011, S. 484) Prozessmanagement folgendermaßen:

> Prozessmanagement umfasst die ganzheitliche Planung, Steuerung und Kontrolle der betrieblichen Abläufe im Hinblick auf deren Kosten, Zeit und Qualität. Ziel ist die bestmögliche Erfüllung der Kundenanforderungen durch das Prozessergebnis.

"Die Besonderheit des Prozessmanagements ist die durchgehende Orientierung am Kunden, in deren Rahmen auch interne Kunden-Lieferanten-Beziehungen berücksichtigt werden…Ergänzt wird das Konzept durch laufende Verbesserungen, die sinnvollerweise für die Mitarbeiter mit entsprechenden Anreizen verbunden sind" (Dillerup und Stoi, 2011).

Es ist aber nicht ausreichend sich nur am Kunden zu orientieren. Dies ist nur ein wichtiger Aspekt. Das Geschäftsprozessmanagement sollte neben den Kundenbedürfnissen auch die strategischen Ziele des Unternehmens berücksichtigen (siehe Abbildung 4). "Dazu dienen Prozessführung, Prozessorganisation und Prozesscontrolling. Sie schaffen die Voraussetzungen für die Zielerreichung und Optimierung der Geschäftsprozesse." (Schmelzer und Sesselmann, 2013, S. 8)

Abbildung 4: GPM Ausrichtung an Kunde und Strategie

Schmelzer und Sesselmann (2013, S.15) gehen noch weiter und haben das Geschäftsprozessmanagement zusammenfassend mit folgenden Eigenschaften charakterisiert: Prozessorientiert, Strategieorientiert, Kundenorientiert, Wertschöpfungsorientiert, Performanceorientiert, Mitarbeiterorientiert, Lernorientiert und Kompetenzorientiert.

Zur Muehlen und Ho (2006) fassen unterschiedliche Definitionen des Geschäftsprozessmanagements zusammen. Danach ist die zentrale Aufgabe des Geschäftsprozessmanagements die verschiedenen Komponenten eines Prozesses (Input, Output, Ressourcen, Prozessstruktur und Prozessziele) zueinander bündig auszurichten. Wenn solch eine Ausrichtung erreicht wird, dann sollte sich die allgemeine Effizienz der Prozesse im Unternehmen steigern und sowohl Qualität als auch Quantität des Outputs sollten wesentlich verbessert werden.

Diese Ausrichtung wird aber selten durch eine einmalige Prozessoptimierung erreicht. Um dies zu erreichen sollte ein iteratives Verfahren eingeführt werden, in Form eines kontinuierlichen Prozessmanagement Kreislaufs (siehe Abbildung 5).

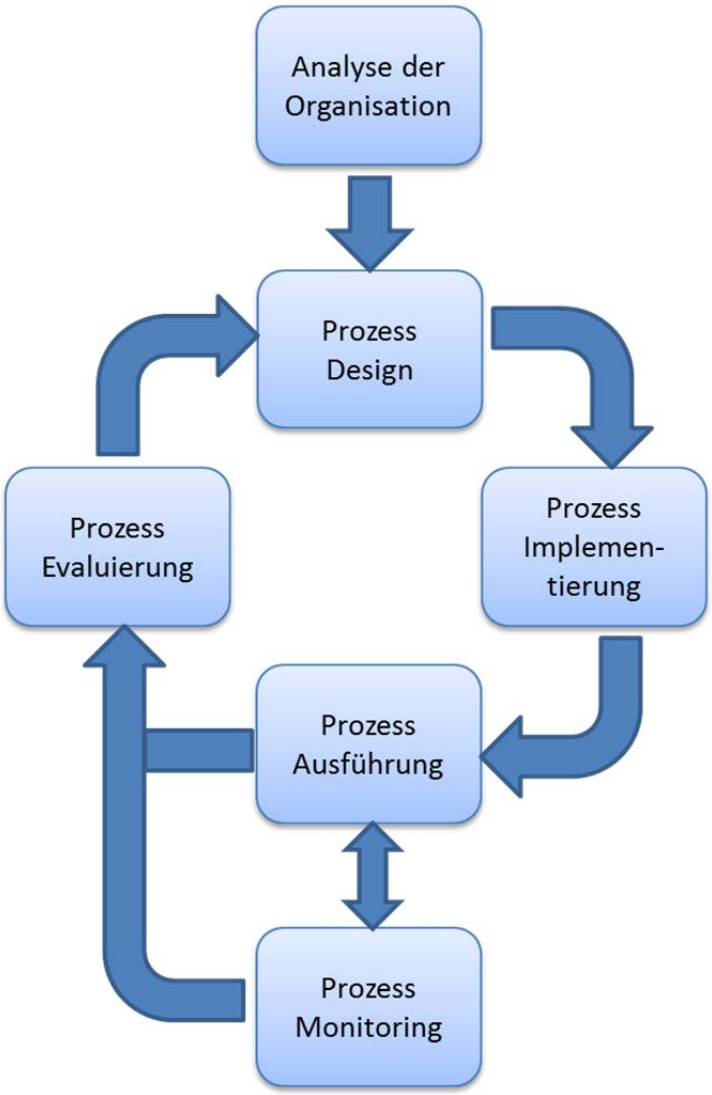


Abbildung 5: GPM Kreislauf (angelehnt an zur Muehlen und HO, 2006)

2.2 Prozessorientierte Organisationen

Unternehmen wollen sehr schnell auf den Markt und auf wechselnde Kundenbedürfnisse reagieren können und die Fähigkeit haben, qualitativ hochwertige Produkte in kurzer Zeit zu liefern, um Konkurrenzfähig zu bleiben (Dräger/Rößler, 2012). Dies können prozessorientierte Organisationen. Schmelzer und Sesselmann (2013, S.30) führen eine Studie an, laut der "beeinflusst der Grad der Prozessorientierung die Höhe der Effizienz von Organisationen. Je höher der Grad der Prozessorientierung ist, desto höher ist die Organisationseffizienz."

Heutzutage sind die meisten Organisationen aber noch funktionsorientiert aufgebaut. "Das bedeutet, dass zusammenhängende Funktionen in einer Einheit gebündelt werden, z.B. die Buchhaltung, die Personalabteilung oder die Kundenabteilung. Die Geschäftsprozesse stehen orthogonal zu dieser Struktur" (Weilkiens, Weiss, Grass, 2010, S. 63). Dabei konzentriert sich der Aufbau auf Spezialisierung und Aufgabenteilung. Dies hat den Ur-

sprung in Taylors Theorie der arbeitsteiligen Produktion. Becker, Kugeler und Rosemann (2012, S. 6) fassen dies wie folgt zusammen: "die Aufbauorganisation beinhaltet die Gliederung der Unternehmung in Teilsysteme (z.B. Abteilungen, Divisionen, Stellen) und die Zuordnung von Aufgaben zu diesen Teilsystemen."

Häufig führen der funktionale Aufbau einer Organisation und die Ausrichtung der Abläufe daran zu einer Vielzahl an Übergabepunkten an Funktionsgrenzen. Diese führen wiederum zu einem erheblichen Aufwand an Kommunikation und Koordination und damit zu einer unflexiblen und zeitraubenden Arbeitsabwicklung. Auch die funktionsübergreifende Betrachtung von Abläufen gerät dort leicht in den Hintergrund.

Die **Prozessorientierung** kann die Zahl der Schnittstellen erheblich reduzieren, da Teilprozesse bei einem Bearbeiter oder einer Organisationseinheit zusammengefasst werden (Dillerup und Stoi, 2011). Die Mitarbeitermotivation wird dabei erhöht, da der Gesamtüberblick über die Abläufe (Leistungszusammenhang) behalten wird und der Mitarbeiter durch abgeschlossene Aufgaben Erfolgserlebnisse erhält.

Auch Dräger und Rößler (2012) weisen darauf hin, dass die Prozessorientierung nicht nur Durchlaufzeiten und Kosten optimiert, sondern auch die Mitarbeitermotivation verbessert wird.

Bei der Prozessorientierung werden Geschäftsprozesse vom Kunden aus über die gesamte Prozesskette im Unternehmen (die Auftragsabwicklung) und wieder bis zum Kunden hin definiert. Sachlich und fachlich zusammenhängende Aktivitäten werden ganzheitlich zusammengefasst und auf einen oder wenige beteiligte Mitarbeiter übertragen.

Es ist nicht einfach eine prozessorientierte Organisation zu werden und es werden wohl jedem bei der Neuausrichtung einige Schwierigkeiten begegnen. Weilkiens, Weiss und Grass (2010) weisen darauf hin, dass einige Faktoren wichtig sind, um erfolgreich zur Prozessorientierung zu gelangen. Wichtig ist z.B., dass die Werte der Organisation entsprechend angepasst werden und sie die erfolgreiche Arbeit in Prozessen fördern. Auch Vision und Mission sollten so gestaltet sein, dass sie die Geschäftsprozesse als zentrales Element der Organisation fördern. Ebenso muss die Struktur entsprechend angepasst werden. "Die Geschäftsprozesse benötigen einen Prozessverantwortlichen, was unter Umständen eine neue Rolle in der Organisation ist" (Weilkiens, Weiss, und Grass, 2010, S. 65).

3 Grundlagen Governance, Risiko, Compliance

Governance, Risiko und Compliance (GRC) sind eng miteinander zusammenhängende und verwobene Themen. In diesem Kapitel werden erst die einzelnen Themen vorgestellt und definiert. Anschließend wird das GRC-Management beschrieben und definiert. Das GRC-Management beinhaltet die einzelnen Themen Governance, Risiko und Compliance, ist aber durch die entstehenden Synergien und die holistische Betrachtungsweise in der Regel mehr als nur die Summe seiner Teile.

3.1 Governance

Corporate Governance bedeutet direkt übersetzt zu Deutsch *Unternehmensführung* oder *Unternehmensverfassung* (Romeike, 2008). Allerdings wird der Begriff im Sprachgebrauch nicht nur als Unternehmensführung verstanden, sondern eher normativ eingesetzt. Daher wird in den Definitionen nicht nur das "Was" sondern meist auch das "Wie" mit einbezogen.

So beschreiben z.B. Schmelzer und Sesselmann (2013, S. 38) Governance als gute und verantwortungsvolle Unternehmensführung und -kontrolle: "Ziel der Governance ist es, eine verantwortungsvolle zielgerichtete und transparente Führung und Überwachung zu gewährleisten."

Corporate Governance gibt demnach dem Management einer Organisation Überblick und Ausrichtung. Sie gibt einen Rahmen vor, wie Prozesse gelenkt werden sollen und gibt Richtlinien und Regeln vor, wie sich das Unternehmen und die Mitarbeiter 'benehmen' sollen (siehe Abbildung 6).

Ein weiteres Ziel der Corporate Governance ist die Festlegung der Beziehung zwischen Unternehmensführung und Eigentümer. "Nach herrschender Meinung war und ist das Auseinanderfallen von Eigentum und Kontrolle das Kernproblem von Corporate Governance" (Menzies, 2009, S. 4). Die Unternehmensführung soll im Sinne und zur allgemeinen Nutzen der Shareholder handeln. Damit sichert Corporate Governance "die Existenz von Unternehmen und wirkt sich positiv auf den Unternehmenswert aus" (Menzies, 2009, S. 4).

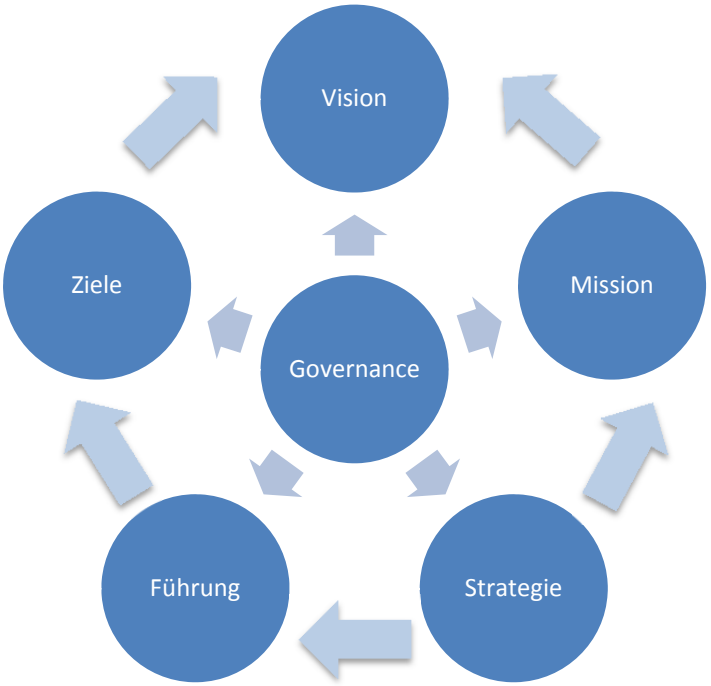


Abbildung 6: Governance

Verschiedene Leitlinien und Regelwerke beschreiben wie in einer Organisation gute Unternehmemsführung (Corporate Governance) aussehen sollte. Dabei gibt es unterschiedliche Zielrichtungen (Krems, 2012):

- Eine gute Unternehmensführung im Sinne der Eigentümer und der Öffentlichkeit
- Langfristigen Erfolg durch zusätzliches Einbeziehen von weiteren Stakeholdern (wie z.B. Mitarbeitern)
- Einen umfassenden Ansatz der auch gesellschaftliche und kulturelle Verantwortung mit einbezieht.

Einen internationalen Standard geben die Leitlinien der OECD für Corporate Governance, die relativ umfassend sind. Die OECD (2004) hat die große Bedeutung von Corporate Governance erkannt und sagt, dass sie ein Schlüssel zum Unternehmenserfolg und -wachstum ist und sie das Vertrauen von Investoren fördert. Folgendes findet sich in den OECD Grundsätzen zur Corporate Governance:

"Sie betreffen das ganze Geflecht der Beziehungen zwischen dem Management eines Unternehmens, dem Aufsichtsorgan, den Aktionären und anderen Unternehmensbeteiligten (Stakeholder). Die Corporate Governance liefert auch den strukturellen Rahmen für die Festlegung der Unternehmensziele, die Identifizierung der Mittel und Wege zu ihrer Umsetzung und die Modalitäten der Erfolgskontrolle." (OECD, 2004, S. 11)

Der deutsche Corporate Governance Kodex ist für börsennotierte Unternehmen verpflichten und gilt als Empfehlung für alle anderen. Er wird von der Regierungskommission Deutscher Corporate Governance Kodex verabschiedet und regelmäßig aktualisiert und

er besitzt über die Entsprechenserklärung gemäß § 161 AktG eine gesetzliche Grundlage (DCGK, 2015).

Der deutsche Kodex bezieht sich auf die Unternehmensinteressen (also die gute Unternehmensführung im Sinne der Eigentümer) und geht damit weniger weit, als die OECD Leitlinien (Krems, 2012). Er enthält verbindliche Regelungen, Soll-Regeln und Empfehlungen. Der DCGK "definiert den rechtlichen Ordnungsrahmen für die Leitung und Überwachung eines Unternehmens bzw. empfiehlt Grundsätze für eine optimale Unternehmensführung sowie eine optimale Überwachung eben dieser Führung" (Romeike, 2008, S 33).

Laut Krems (2012) sind die japanischen Leitsätze der Keidanren Charter for Good Corporate Behavior ein sehr umfassendes Regelwerke (Einbeziehung aller Stakeholder und gesellschaftlicher und kultureller Verantwortung), die auch den Richtlinien eines umfassenden Qualitätsmanagement TQM entsprechen.

Es existiert keine einheitliche Definition für Corporate Governance. Viele Unternehmen definieren ihre Corporate Governance in ihren Corporate-Governance-Berichten. Dabei werden ein Verhaltensrahmen für die Leitungsorgane und bei einer Aktiengesellschaft das Zusammenwirken von Leitungs- -und Überwachungsorgan definiert. Außerdem sollen das Vertrauen von Investoren, Kunden, Mitarbeiter, und der Öffentlichkeit in die Unternehmensleitung und Überwachung gefördert werden (Romeike, 2008).

Zur Corporate Governance gehört ebenfalls ein internes Überwachungssystem, das unternehmensinterne Kontrollsysteme und das Risikomanagement überprüft, ob sie umgesetzt wurden und ob sie zielführend sind. (Fischermanns, 2014)

Streck und Binnewies (2009) beleuchten den Begriff Corporate Governance aus Richtung der Regelerstellung. Für sie ist Corporate Governance ein Regelwerk für die Unternehmensleitung. Es beinhaltet die Gesamtheit der organisatorischen und inhaltlichen Anordnungen für die rechtlich einwandfreie, verantwortungsvolle und zielgerichtete Führung und Überwachung des Unternehmens. Corporate Governance·Regeln können sowohl verpflichtend als auch unverbindlich gestaltet sein.

3.1.1 Governance und Prozessmanagement

Governance gibt auch den Rahmen für das Prozessmanagement vor. Weilkiens, Weiss und Grass (2010, S. 147) definieren folgendermaßen: "Die *Corporate Governance* ist die Menge der Prozesse und Vorgaben, die die Einheiten eines Unternehmens führen, steuern und verwalten. Sie leitet sich aus den Zielen und dem Umfeld des Unternehmens ab und wird maßgeblich durch Vorgaben beeinflusst." Diese Definition nimmt direkten Bezug auf die Führungsprozesse eines Unternehmens und betont die Bedeutung, die Führungsprozesse (siehe Kapitel 2.1.3) an den Richtlinien und der Strategie auszurichten, die in der Corporate Governance beschrieben sind. Bei gemeinsamer Ausrichtung von Corpora-

te Governance und Prozessmanagement, werden durch die Corporate Governance die Führungsprozesse beschrieben.

Eine weitere Komponente der Corporate Governance ist die Process Governance. "Sie umfasst die unternehmensweit gültigen Regeln, Vorschriften, Werte und Grundsätze bezogen auf Führung, Organisation, Kontrolle, Steuerung und Optimierung der Geschäftsprozesse und das gesamte Geschäftsprozessmanagementsystem." (Schmelzer und Sesselmann, 2013)

3.2 Risikomanagement

In dieser Arbeit geht es nicht um die Risiken, die mit GPM-Projekten verbunden sind, sondern um das allgemeine Risikomanagement einer Organisation und wie dieses bei der Prozess-orientierten Ausrichtung eines Unternehmens in das GPM integriert werden kann.

3.2.1 Risiken

Risiken sind alle internen und externen Ereignisse und Entwicklungen, die das Erreichen der Unternehmensziele gefährden. Hierzu zählen nicht nur direkt monetär fassbare Risiken, wie etwa Verluste eines Unternehmensteils oder ein Brandschaden, sondern auch qualitative Risiken wie sie etwa ein Rufschaden oder ein Attraktivitätsverlust als Arbeitgeber darstellen.

Risiken können auch mathematisch ausgedrückt werden, als die Wahrscheinlichkeit für das Auftreten von Verlust oder Gewinn multipliziert mit der entsprechenden Gewinn- bzw. Verlustgröße (zur Muehlen und Ho, 2006).

Das PMI (Project Management Institute) definiert Risiko als "an uncertain event or condition that, if it occurs, has a positive or negative effect on a project’s objectives" (PMI; 2015).

Rieke und Winkelmann (2008) haben festgestellt, dass in der wirtschaftswissenschaftlichen Literatur zwei unterschiedliche Auffassungen zum Risikobegriff vorherrschen. Sie unterscheiden in die "wirkungsbezogene Begriffsauffassung" und die "ursachenbezogene". "Die *wirkungsbezogene* Begriffsauffassung fokussiert auf die möglichen Auswirkungen und beschreibt das Risiko als Möglichkeit der Zielabweichung" und "die ursachenbezogene Begriffsauffassung setzt am Punkt der Risikoentstehung an und stellt die Entscheidung, die durch ein Informationsdefizit geprägt ist, in den Vordergrund der Betrachtung." Diese beiden Ausrichtungen widersprechen sich aber nicht. Sie können im Gegenteil miteinander verknüpft werden.

3.2.2 Gesetzliche Grundlage und Definition Risikomanagement

Es gibt zahlreiche gesetzliche Grundlagen für das Risikomanagement. Dazu zählen Basel II (Banken), Solvency II (Versicherungen), der Sarbanes-Oxley Act (amerikanische Rechtsprechung), das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) und der Deutsche Corporate Governance Kodex (Rieke und Winkelmann, 2008).

Der § 91 Abs. 2 AktG bestimmt: "Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand des Unternehmens gefährdende Entwicklungen früh erkannt werden."

Durch systematisches Risikomanagement sollen unternehmerische Risiken erkannt, bewertet und berichtet werden und es sollen potenzielle Risiken durch Kontrollmaßnahmen in dem Maße minimiert werden, dass deren Eintritt das Erreichen der Unternehmensziele nicht gefährdet. Risikomanagement soll dabei den Spielraum der Unternehmung nicht einengen (verstanden als Vermeidung aller risikoreichen Aktivitäten), sondern es sollen Chancen bei transparenten und beherrschbaren Risiken konsequent genutzt werden können. Ziel ist es nicht, "das natürliche Risiko unternehmerischen Handelns auf der Tatsache eines unvollständigen Informationsstandes, also der Unsicherheit bzw. der Ungewissheit über zukünftige Ereignisse aufgrund unsicherer oder fehlender Daten zu eliminieren, sondern Prozessrisiken zu analysieren, zu kontrollieren und darüber zu berichten" (Becker, Kugeler und Rosemann, 2012, S. 522).

Zu den relevanten Risiken gehören sowohl Compliance-Themen (siehe 3.3), soweit daraus Risiken entstehen, sowie alle weiteren internen und externen Unternehmensrisiken.

Risikomanagement dient der Identifikation, Bewertung, Steuerung und Überwachung (inklusive Dokumentation) von Risiken. "Diese Phasen werden in einem iterativen Prozess durchlaufen, die Ergebnisse des Risikocontrollings werden darüber hinaus bei der Definition der Risikomanagementstrategie rückkoppelnd berücksichtigt." (Becker, Kugeler und Rosemann, 2012, S. 520)

Die verschiedenen Phasen dieses Risikomanagement-Kreislaufs (siehe Abbildung 7) werden begleitet durch eine Risikopolitik, Prozessüberwachung und einer Risikokommunikation (Gabler, 2015).

Durch die *Identifikation* werden alle aktuellen und zukünftigen Risiken gesammelt. Die *Bewertung* erfolgt meistens indem die Eintrittswahrscheinlichkeit und die erwartete Schadenshöhe bei Eintritt multipliziert werden. Die *Steuerung* findet Möglichkeiten, um auf das identifizierte und bewertete Risikospektrum ihm Rahmen der festgelegten Risikopolitik zu reagieren "Dabei stehen einer Unternehmung grundsätzlich vier verschiedene Steuerungsmöglichkeiten zur Auswahl: Vermeidung mit gleichzeitigem Geschäftsverzicht, Verminderung, Überwälzung z.B. auf eine Versicherung oder das Selbsttragen des Risikos." (Gabler, 2015)

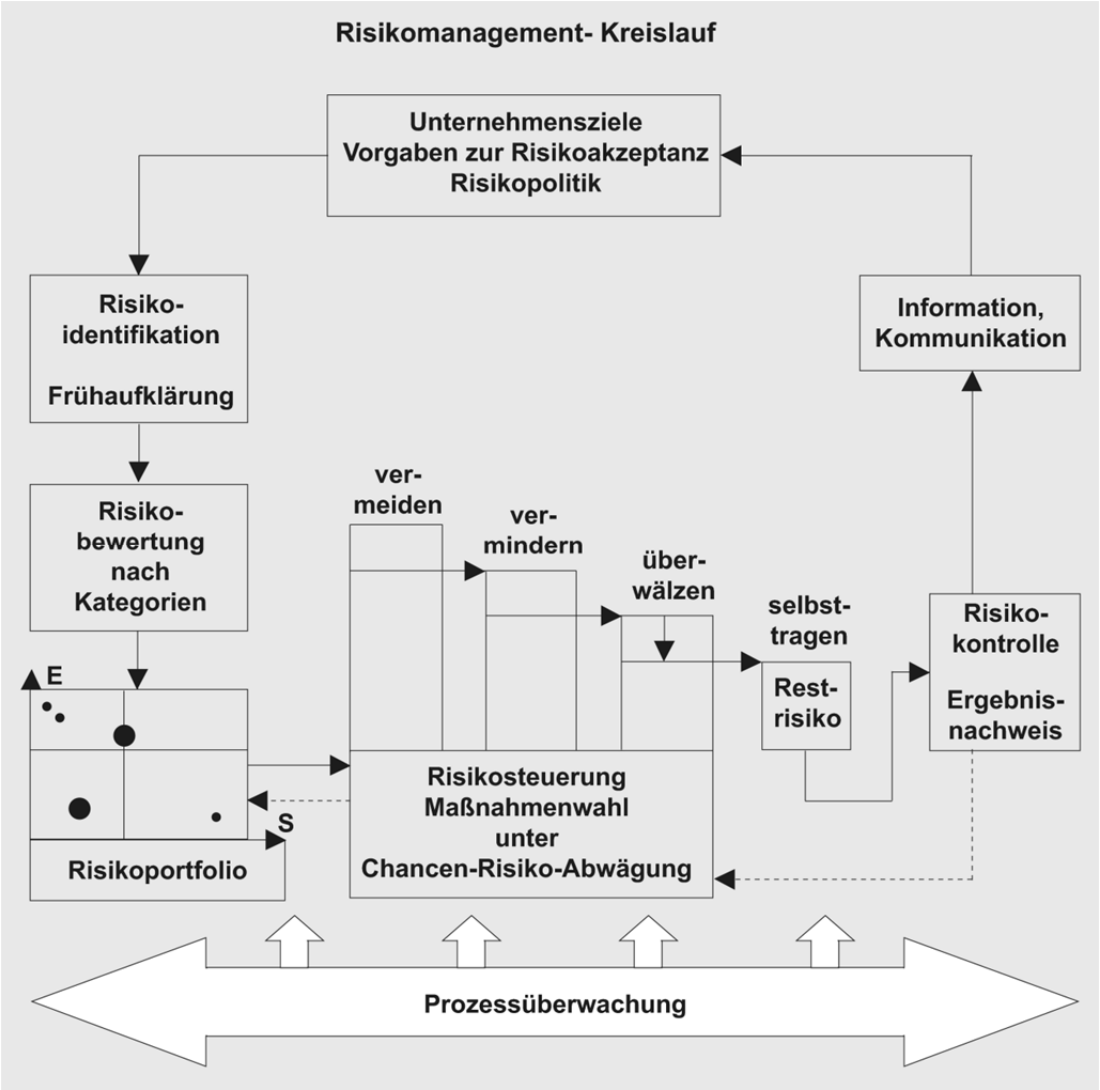


Abbildung 7: Risikomanagement (Gabler, 2015)

3.2.3 Risikomanagement und Prozessmanagement

Effektives Risikomanagement kann nur in Verbindung mit dem Prozessmanagement stattfinden. So ist es z.B. eine Aufgabe des Risikomanagers die identifizierten Risiken innerhalb der Organisation zu kommunizieren. In einer Prozess-orientierten Organisation kann der Risikomanager an die Prozessverantwortlichen die für sie relevanten Risiken weitergeben und diese können dann alle am Prozess beteiligten Mitarbeiter informieren. (Rieke und Winkelmann, 2008)

Rieke und Winkelmann (2008) haben festgestellt, dass auch vor dem Hintergrund der aktuellen Gesetzgebung (KonTraG, Sarbanes.Oxley bzw. COSO, Basel II) Prozessmodellanalysen zur Risikoidentifizierung notwendig sind bzw. teilweise schon direkt darauf verweisen.

Auch bei externer Prüfung des Risikomanagements eines Unternehmens (z.B. nach IDW-Standard) bietet sich die Verwendung von Prozessmodellen an. "Die Verwendung von

Prozessmodellen bietet sich hier an, da die Kontrollmaßnahmen im prozessualen Kontext präsentiert werden und damit besser nachvollziehbar werden. Die Prozessmodelle können damit Bestandteil des Risikomanagementhandbuchs werden und dieses sinnvoll und zielführend erweitern" (Rieke und Winkelmann, 2008, S. 347).

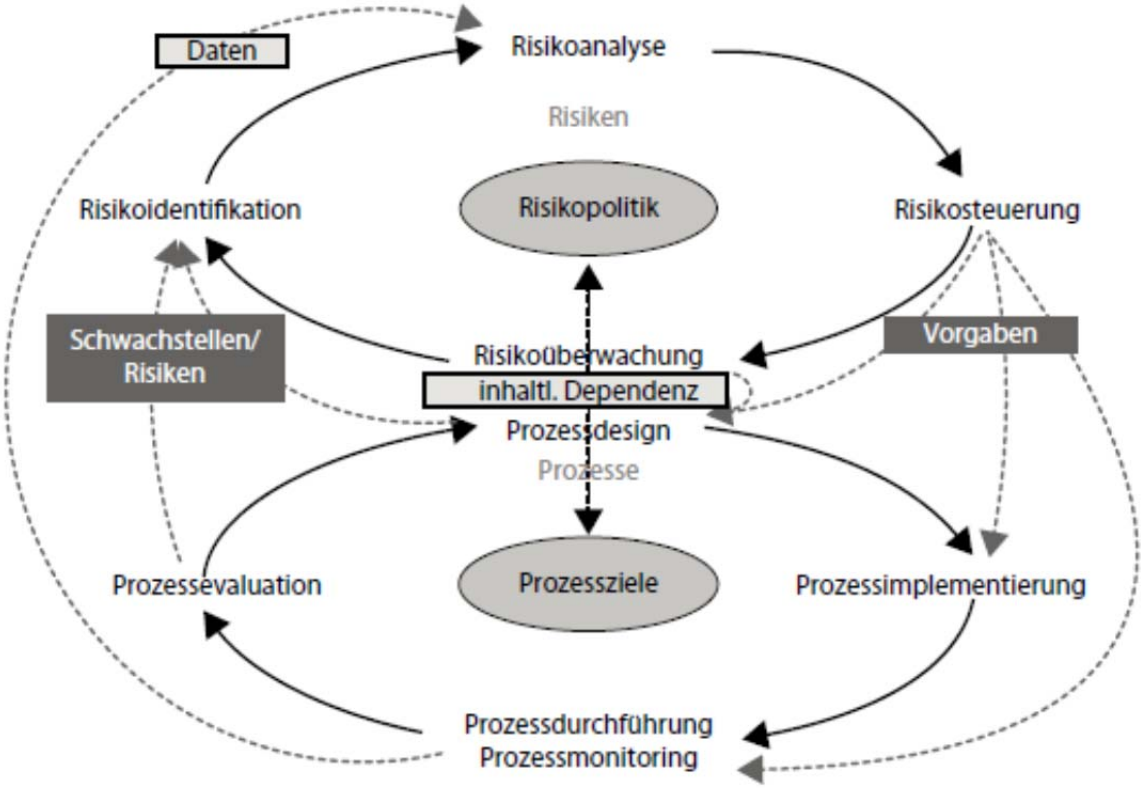


Abbildung 8: Abhängigkeiten Prozess- und Risikomanagement (Rieke und Winkelmann, 2008)

3.3 Compliance

Im Grunde ist es Allgemeinwissen, dass Unternehmen, ihre Leitungsorgane und ihre Mitarbeiter sich an das geltende Recht halten müssen. "Dass dies jedoch in der Praxis nicht selbstverständlich ist, zeigt sich anhand verschiedener in jüngerer Vergangenheit bekannt gewordener Fälle der Wirtschaftskriminalität in deutschen Unternehmen, anhand von Kartellverstößen, die durch Rekordbußgelder sanktioniert wurden oder diversen Unternehmenskrisen, zu denen es durch Gesetzesverstöße gekommen ist, an denen teilweise die Unternehmensleitungen in erheblicher Weise beteiligt waren." (Romeike, 2008, S. 19)

Schon allein wegen drohenden juristischen und finanziellen Nachteilen sowie Reputationsschäden bei Regelverstößen, muss sich jede Unternehmensleitung mit Compliance beschäftigen. "Das Einhalten von globalen Regeln und Standards ist heute eine Grundvoraussetzung dafür, dass Unternehmen Geschäfte betreiben und am Markt auftreten dürfen" (Menzies, 2009, S. 3).

Der Begriff **Compliance** kommt aus dem Englischen (to comply with something = mit etwas übereinstimmen) und beschreibt im weitesten Sinne Regeltreue oder Regelkonformität. Im betriebswirtschaftlichen Sinn steht Compliance für die Einhaltung sämtlicher für das jeweilige Unternehmen relevanten Compliance-Regelungen.

Einige Vorstände und Geschäftsführer haben aber bereits auch erkannt, dass Compliance nicht nur präventiv Risiken aus Regeverstößen vorbeugt, sondern sie "erkennen nicht selten in einem funktionierenden Compliance-Management auch den strategischen Vorteil gegenüber dem Wettbewerb" (Wecker und van Laak, 2009, S. 33). Dies ist nicht nur der Fall, weil Unternehmen durch rechtmäßiges Handeln vermeiden auf die sog. Schwarze Liste zu kommen (und damit von gewinnbringenden Geschäften ausgeschlossen werden), sondern auch weil viele Unternehmen eher mit Partnern Geschäfte machen, bei denen sie nicht mit dem Risiko von Regelverstößen rechnen müssen, das auch auf ihre eigene Reputation Einfluss nehmen würde.

Eine weitere Definition für Compliance gibt Krügler (2011, S. 50): „Der Begriff Compliance steht für die Einhaltung von gesetzlichen Bestimmungen, regulatorischer Standards und Erfüllung weiterer, wesentlicher und in der Regel vom Unternehmen selbst gesetzter ethischer Standards und Anforderungen.“

Compliance-Regelungen sind die Gesamtheit aller Regelungen im Unternehmen. Sie sollen sicherstellen, dass gesetzliche und individuelle Vorgaben von allen Mitarbeitenden eingehalten werden. Bei den individuellen Vorgaben handelt es sich um Regelungen, die aus strategischen, kundenrelevanten oder gesellschaftlichen Gründen als Regelung vorgeschrieben werden. Menzies (2009) geht noch weiter und beschreibt Compliance nicht nur als die Einhaltung von Regelungen, sondern auch als "die Erfüllung weiterer wesentlicher Anforderungen der Stakeholder" und "Compliance trägt dazu bei, die Beständigkeit des Geschäftsmodells, das Ansehen in der Öffentlichkeit und die finanzielle Situation eines Unternehmens zu verbessern" (S. 2).

Im Jahr 2002 hat das Bundesministerium der Justiz den Deutschen Corporate Governance Kodex (DCGK) für börsennotierte Unternehmen erstmals veröffentlicht. Der Kodex unterstreicht die Verantwortung des Vorstands, für die Einhaltung gesetzlicher Bestimmungen und unternehmensinterner Richtlinien zu sorgen. Dies wird im Kodex (DCGK, 2015) unter Ziffer 4.1.3 wie folgt definiert: "Der Vorstand hat für die Einhaltung der gesetzlichen Bestimmungen und der unternehmensinternen Richtlinien zu sorgen und wirkt auf deren Beachtung durch die Konzernunternehmen hin (Compliance)." Auch für nicht börsennotierte Unternehmen wird die Einhaltung des Kodex empfohlen.

Compliance beschränkt sich aber nicht nur auf die Einhaltung von Regeln und die Rechtstreue eines Unternehmens, "sondern umschreibt die Summe der organisatorischen Maßnahmen eines Unternehmens, mit denen gewährleistet werden soll, dass sich die Geschäftsleitung wie auch die Mitarbeiter des Unternehmens rechtmäßig verhalten" (Wecker

und van Laak, 2009, S.31). Diese Compliance-Organisation wird mit einem Compliance-Management -System abgebildet.

3.3.1 Compliance-Management-System

Die Unternehmensleitung hat die Pflicht für die Einhaltung der Vorgaben der Rechtsordnung zu sorgen. Rechtsquellen dazu sind neben der gesellschaftsrechtlichen Legalitätspflicht auch § 130 des Ordnungswidrigkeitengesetzes. Um dies sicherzustellen und um sinnvolle interne Regelungen zu erstellen und transparent zu machen, wird in vielen Unternehmen ein Compliance-Management-System (CMS) eingeführt.

Das CMS umfasst alle Maßnahmen und Programme, um regelkonformes Verhalten im Unternehmen zu fördern. Es ist ein integraler Bestandteil der Corporate Governance. Im Grunde ist es ein System, das die Einhaltung von internen und externen sowie verpflichtenden und freiwilligen Vorgaben sicherstellt.

Unter einem **Compliance-Management-System (CMS)** versteht man die Organisation, Dokumentation, Kommunikation und Überwachung von Maßnahmen, welche die Einhaltung von Regelungen systematisch gewährleisten sollen. Die Compliance Programme in einem solchen System haben eine Präventivfunktion. "Durch sie sollen problematische Sachverhalte und Strukturen vermieden, frühzeitig aufgedeckt und potentielle Verstöße möglichst schon im Vorfeld erkannt werden" (Romeike, 2008).

Compliance-Systeme sollen Unternehmen vor Compliance-Risiken schützen. Diese sind Risiken, die durch Verstöße gegen interne oder externe Regelungen entstehen, bei denen große wirtschaftliche Schäden entstehen können. Dabei geht es nicht darum, Mitarbeiter auf Gesetzestreue zu überwachen. Dies sollte selbstverständlich sein. Es geht eher darum, Gesetze und Regeln zu identifizieren, die für das Unternehmen besonders wichtig und besonders risikorelevant sind und diese den Mitarbeitern transparent zu machen. Einen Überblick über die Instrumente eines CMS liefert Wieland (2008), zu sehen in Abbildung 9.

Compliance-Issues	• Korruption • Kartellrecht • Insiderhandel	• Geldwäsche • Umweltrecht • Exportkontrolle	• Vermögensschädigung • Arbeits- und Sozialstandards • Umgang mit Eigentum		
CMS	**Strategie**	**Organisation**	**Leitlinien**	**Kommunikation**	**Kontrolle**
Instrumente	Grundwerte-erklärung Mission-, Vision-, Values-Statement Code of Ethics Compliance Risk Assessment	Chief Compliance Officer Compliance Office Compliance Organisation Ombudsperson Linien-verantwortung Personalabteilung Helpline Hnweisgeber-system	Kartell-rechtsrichtlinie Personalauswahl und Karriereplanung Geschenke-richtlinie Richtlinie Exportkontrolle Lieferanten-auswahl und -bewertung	Schulungen Intranet/Internet Web-based Training Broschüre Mitarbeiter-gespräch Reporting Notfall-management	Dokumentation Monitoring/ Selbstbewertung Compliance-Audits (intern/extern) Detection-Audits Sanktion Zusammenarbeit mit Behörden

Abbildung 9: Instrumente CMS (Wieland, 2008)

Seit März 2011 gibt es einen Prüfungsstandard des IDW, der IDW PS 980. Damit wurden erstmals durch das IDW Grundelemente eines Compliance-Management-Systems definiert. Mit Hilfe des Standards werden Konzeption, Angemessenheit, Implementierung und Wirksamkeit der Elemente (siehe Tabelle 1) eines CMS geprüft.

Der IDW PS (2011, S. 3) definiert ein Compliance Management System als "die auf der Grundlage der von den gesetzlichen Vertretern festgelegten Ziele eingeführten Grundsätze und Maßnahmen eines Unternehmens […], die auf die Sicherstellung eines regelkonformen Verhaltens der gesetzlichen Vertreter und der Mitarbeiter des Unternehmens sowie ggf. von Dritten abzielen, d.h. auf die Einhaltung bestimmter Regeln und damit auf die Verhinderung von wesentlichen Verstößen (Regelverstöße)."

Seit Dezember 2014 gibt es einen globalen Leitfaden zur Gestaltung von CMS, den ISO 19600 "Compliance Management Systems". Dieser Leitfaden unterstützt Unternehmen bei der Implementierung, Umsetzung, Bewertung, Erhaltung und Verbesserung eines CMS.

Compliance Element	**Beschreibung**
Compliance-Kultur	Grundeinstellung und Verhaltensweisen des Managements sowie die Definition der Rolle der Aufsichtsorgane

Compliance-Ziele	Festlegung der relevanten Teilbereiche und der in den Teilbereichen einzuhaltenden Regeln.
Compliance-Organisation	Festlegung von Rollen und Verantwortlichkeiten sowie Aufbau- und Ablauforganisation im CMS als integraler Bestandteil der Unternehmensorganisation
Compliance-Risiken	Festlegung von Compliance-Risiken unter Berücksichtigung von Compliance-Zielen. Einführung von Verfahren zur systematischen Risikoerkennung und -berichterstattung.
Compliance-Programm	Auf Grundlage der Compliance-Risiken erfolgt die Festlegung von Grundsätzen und Maßnahmen zur Begrenzung oder Vermeidung von Compliance-Verstößen.
Compliance-Kommunikation	Information der Mitarbeiter über das Compliance-Programm sowie die damit verbundenen Aufgaben und Rollen.
Compliance-Überwachung und -Verbesserung	Überwachung der Angemessenheit und Wirksamkeit des CMS sowie ggf. Verbesserung bez. Beseitigung festgestellter Mängel.

Tabelle 1: Compliance-Elemente (Becker, Kugeler, Rosemann, 2012, S. 532)

3.3.2 Compliance und Prozessmanagement

"Obwohl Compliance in der Praxis oft als abstrakt, komplex und intransparent angesehen wird, ist es in der heutigen Geschäftswelt ein unausweichliches Thema. Durch die Modularisierung der Prozesse und der Individualisierung der IT, kommen neue Herausforderungen auf die Einhaltung der Compliance zu, bedarf es einer erweiterten Herangehensweise zu ihrer Umsetzung und Sicherstellung" (Rieman, 2012). Compliance ist gerade wegen seiner grundsätzlichen Bedeutung für Struktur, Abläufe und Kultur innerhalb einer Organisation keine reine Maßnahme der Geschäftsführung, sondern fordert einen umfassenden Ansatz in modernen Governance-Strukturen und eine enge Verflechtung mit den Prozessen.

Es bestehen enge Zusammenhänge zwischen Compliance und Prozessmanagement. Das Prozessmanagement unterstützt die Implementierung von Compliance Programmen im Unternehmen. "Viele Compliance-Anforderungen richten sich an Geschäftsprozesse

und sind von diesen zu erfüllen. Das Compliance Management hat die betroffenen Geschäftsprozesse zu adressieren, die prozessspezifischen Anforderungen zu definieren und die Wirksamkeit der Überwachung zu kontrollieren" (Schmelzer und Sesselmann, 2013, S. 39). Es müssen also Prozess im Unternehmen installiert werden, die interne Regelungen und gesetzliche Ansprüche erfüllen, also Compliance-konform sind.

3.4 GRC-Management

Die Bilanzskandale bei Enron und Worldcom, der VW-Abgas-Skandal und andere erschreckende Unternehmensschieflagen ist es zu verdanken, dass Governance, Risikomanagement und Compliance zu sehr aktuellen Themen geworden sind, die bis dahin wenig Beachtung fanden, mit denen sich aber viele Unternehmen danach beschäftigten mussten und weiterhin müssen. Der US-amerikanische Gesetzgeber hat ebenfalls zur Aktualität dieser Themen Beigetragen. Im Rahmen des „Sarbanes-Oxley Act of 2002“ ist dieses Themengebiet in das Interesse der breiten Öffentlichkeit gerückt.

Auch in Deutschland gibt es seit 2002 Regelungen von öffentlicher Seite, den deutschen Corporate Governance Kodex. "Der Deutsche Corporate Governance Kodex stellt wesentliche gesetzliche Vorschriften zur Leitung und Überwachung deutscher börsennotierter Gesellschaften dar und enthält in Form von Empfehlungen und Anregungen international und national anerkannte Standards guter und verantwortungsvoller Unternehmensführung." (DCGK; 2015)

Diese Entwicklungen haben den öffentlichen Meinungsbildungsprozess dahin gehend beeinflusst, dass internationaler Konsens hinsichtlich des Erfordernisses einer „guten“ Corporate Governance besteht.

Compliance und Corporate Governance stehen in enger Verbindung zueinander (zB: comply or explain) und Compliance wiederum verlangt Risikomanagement, um daraus entsprechende Regelungen abzuleiten. Governance wiederum gibt Orientierung für die Risiko-Entscheidungen und Risikomanagement liefert wichtige Grundlagen für die Risiko-Toleranz-Richtlinien der Corporate Governance (siehe Abbildung 10).

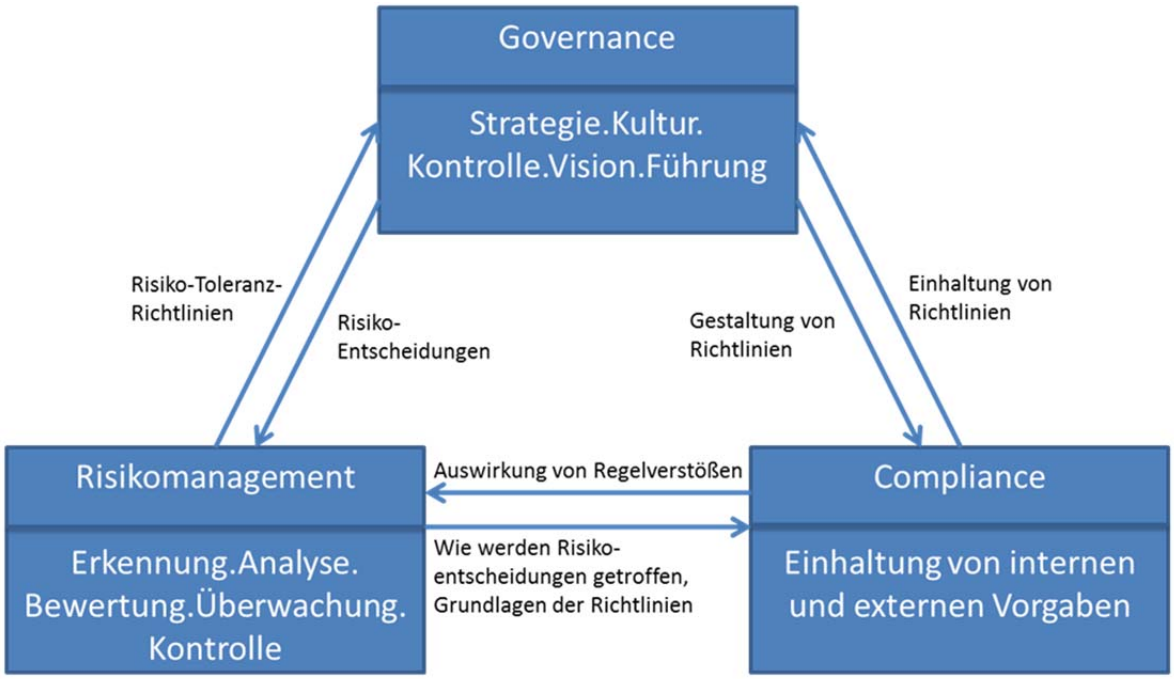


Abbildung 10: Das Zusammenspiel von Governance, Risiko, Compliance

Unter dem Akronym GRC werden in Praxis und Wissenschaft Ansätze diskutiert, wie man die Verflechtungen zwischen den GRC-Disziplinen (Governance, Risk and Compliance) mit den GRC-Komponenten (Strategie, Prozesse, Menschen, Technologie) zielorientiert koordiniert. Das Akronym "GRC" hat die Geschäftswelt in den letzten Jahren immer weiter durchdrungen. Es hat seinen Weg in die verschiedenen Software Produkte, Marketing Folien und Abteilungsnamen in globalen Unternehmen gefunden (Racz, Weippl und Seufert, 2010).

Die einzelnen GRC-Disziplinen, Governance, Risiko und Compliance, sind nicht neu. Das neue an dem GRC-Konzept ist der integrierte Ansatz, der wenn er holistisch in einer Organisation angewendet wird, signifikant zur Wertschöpfung beitragen und zu einem Wettbewerbsvorteil führen kann (PwC, 2005).

Vor allem viele IT-Firmen haben den Begriff GRC geprägt, da sie IT-Werkzeuge anbieten, die die GRC-Disziplinen integriert unterstützen sollen. Damit soll ein reibungsloses ineinandergreifen der GRC-Disziplinen ohne Daten-Schnittstellen möglich werden. "Der Aufbau von Insellösungen im Unternehmen (einerseits Risiko- und andererseits Compliance-Managementsysteme) führt hingegen zu Intransparenzen, Redundanzen und Inhomogenität von Daten" (Weuster, 2014, S.13).

Obwohl viel Geld in die Umsetzung der GRC-Disziplinen investiert wird und sehr viele Stellen in diesem Bereich geschaffen wurden, gab es lange eine breit gefächerte Auswahl verschiedener Definitionen für das GRC-Management. Viele Beratungshäuser und Softwarefirmen publizieren Definitionen, die zur Ihren Produkten und Dienstleistungen passen.

3.4.1 Definition

2010 wurde erstmals eine wissenschaftlich herbeigeleitete und validierte Definition veröffentlicht (Racz, Weippl und Seufert, 2010): "GRC ist ein integrierter, holistischer Ansatz für organisationsweite Governance, Risk und Compliance, der gewährleistet, dass die Organisation sich ethisch und gemäß ihres Risikoappetits sowie interner und externer Vorgaben verhält, ermöglicht durch die Abstimmung von Strategien, Prozessen, Menschen und Technologie, wodurch Effizienz und Effektivität gesteigert werden."

Die Risiken, die durch ein Risiko-Managementsystem identifiziert, bewertet und gesteuert werden, können aus der Nichteinhaltung von gesetzlichen oder internen Regelungen (Compliance) stammen, aus dem alltäglichen Geschäftsbetrieb oder aus IT-Risiken herrühren. Daher ist es für das Risiko-Management notwendig alle Regelungen zu kennen und einzuhalten. Dies ist die Aufgabe des Compliance-Managements. Die Nichteinhaltung von Compliance führt also zu neuen Risiken und aufgedeckte Risiken führen wiederum zu neuen oder optimierten Regelungen.

Durch die Corporate Governance werden das Risikomanagement und das Compliance-Management gesteuert. Sie legt die Verantwortlichketen fest und die Unternehmensziele. Anhand derer und auf Grundlage der Erkenntnisse aus Risiko- und Compliance-Management werden die richtigen Unternehmens-Entscheidungen getroffen.

Dieses Zusammenspiel erfordert eine gemeinsame und abgestimmte Strategie und ein gemeinsames Management führt zu einer gesteigerten Effizienz. Daher rührt die Betrachtung des GRC-Managements. Das Beratungshaus KPMG beschreibt GRC als eine strategische Disziplin: GRC ist ein kontinuierlicher Prozess, der in die Kultur einer Organisation eingebettet ist und der steuert wie das Management Risiken identifiziert und sich dagegen schützt, wie es die Effektivität der internen Kontrollen überwacht und evaluiert und wie es dann auf die Ergebnisse reagiert und Prozesse auf Grund der gewonnenen Erkenntnisse optimiert (Racz, Weippl und Seufert, 2010).

Die Regeln des Systems GRC werden durch die die Compliance-Anforderungen, das Risiko-Management und die Corporate Governance definiert. Unabhängig davon, in welcher Form diese Regeln dokumentiert sind (Regelungen, Zielvereinbarungen, etc.), sind sie doch alle normative Anleitungen, die integriert präsentiert und eingesetzt werden sollten (Racz, Weippl und Seufert, 2010).

Zusammenfassend kann man folgende Ziele des GRC-Managements identifizieren:

- Unternehmensstrategie festlegen, umsetzen und nachhalten
- Governance Strukturen und Entscheidungsprozesse definieren und einhalten
- Zielvorgaben definieren, weitergeben und nachhalten
- Risiken für die Zielerreichung identifizieren, bewerten, steuern und überwachen
- Umfeld mit transparenten Regelungen und Richtlinien schaffen, Regelungen definieren, kommunizieren und nachhalten

3.4.2 Vorteile des integrierten GRC-Managments

Deloitte (2008) beschreibt die Vorteile eines integrierten GRC-Managements folgendermaßen: Verschiedene Funktionen sind auf die gleichen Informationen, Technologien und Prozesse angewiesen. Alle Risiko-Management Aktivitäten werden von den gleichen Regeln gesteuert. Jeder erhält zeitnahen Zugang zu benötigten Informationen, um bessere Entscheidungen treffen zu können und das ganze System ist gestärkt von einer Kultur, die gute Unternehmensführung wertschätzt und die Mitarbeiter dafür belohnt das Richtige zu tun.

Marekfia und Nissen (2009, S. 9) beschreiben ebenfalls Vorteile (Nutzeneffekte) von GRC: "Nutzeneffekte für die internen und externen Stakeholder (GRC-bewusste Unternehmenskultur, höhere Unternehmensreputation, gesteigerter Markenwert), die strategische Ebene (bspw. Flexibilitätssteigerung bei M&M-Aktivitäten, Markteintritt und neuen Produkten sowie Verbesserung der Informationsversorgung), Nutzeffekte für das GPM (bspw. Anregungen zur Geschäftsprozessoptimierung) sowie Nutzen im GRC-Management selbst (bspw. durch synergiebedingte Kostensenkungen)."

3.4.3 GRC und Prozessmanagement

Die operative Umsetzung der Anforderungen der GRC-Disziplinen erfolgt in den Prozessen eines Unternehmens. Diese sind das zentrale Mittel zur Gestaltung von GRC.

Das Prozessmanagement wiederum hat zum Ziel die Prozesse jederzeit flexibel an neue fachliche Anforderungen anzupassen. Dabei nimmt das GRC-Management "eine Schnittstellenfunktion zwischen der strategischen Ebene und der Ableitung der Geschäftsprozesse sowie deren IT-seitiger Implementierung ein" und "es ist mit strategischen Zielen abzustimmen sowie mit den weiteren Managementsystemen, welche GRC beeinflussen" (Marekfia und Nissen, 2009, S. 8), wie z.B. das Geschäftsprozessmanagement. Um das GRC-Management effektiv im Unternehmen zu etablieren, sollte es in diese bestehenden Managementsysteme integriert werden und deren Strukturen, Methoden und Werkzeuge nutzen.

Racz, Weippl und Seufert (2010) haben ein abstraktes Modell zur Grundlage weiterer Forschung zum Thema GRC entwickelt. Dieses hebt die Schlüsselelemente hervor, die bei der Untersuchung des GRC-Konzepts betrachtet werden sollten. Dabei sind auch die Prozesse eines Unternehmens ein wesentlicher Bestandteil (siehe Abbildung 11)

Governance, Risiko-Management und Compliance sind dabei natürlich die Kern-Themen. Jedes dieser Themen besteht, wie auch alle Vorgänge eines Unternehmens, aus vier grundlegenden Komponenten: Strategie, Prozesse, Technologie und Menschen. Der Risikoappetit, die internen Vorgaben und die externen Vorgaben sind die Regeln dieses Systems. Die Kern-Themen, die Komponenten und die Regeln werden nun integriert, holostisch und organisationsweit zusammengebracht. Dabei muss dieses System an den durch GRC gesteuerten und unterstützen Aktivitäten ausgerichtet sein.

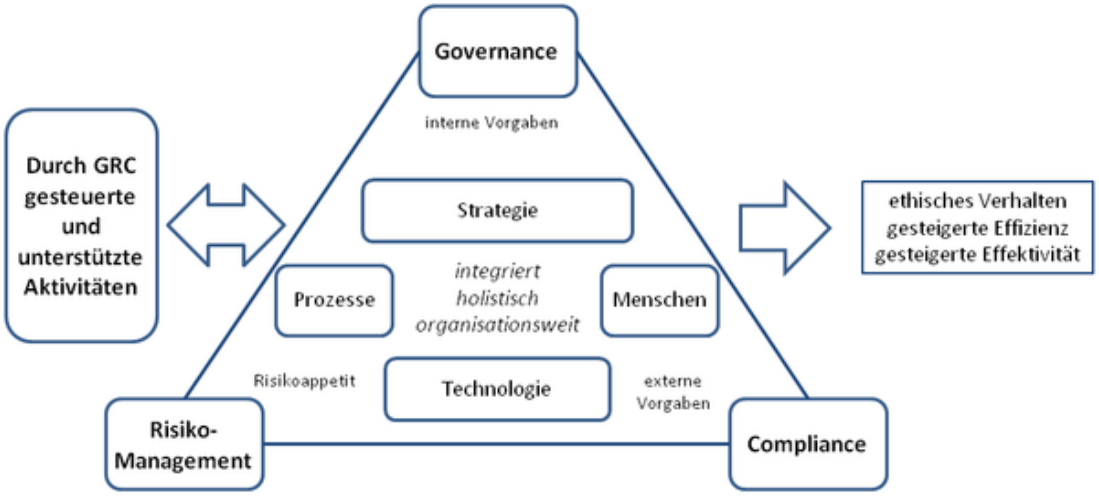


Abbildung 11: Referenzrahmen für integriertes GRC (Racz, Weippl und Seufert, 2010)

Mit diesem Ansatz streben Organisationen danach ihre Ziele des GRC-Systems zu erreichen: sowohl ethisch korrektes Verhalten und fundierte Risikoentscheidungen sowie optimierte Effizienz und Effektivität aller beteiligten Elemente.

Die IT hat ebenfalls einen großen Anteil an der Umsetzung von GRC-Anforderungen. Dies wird durch BPM-Tools und -Systeme unterstützt. Diese stellen eine der Verbindungen von Prozessmanagement mit dem GRC-Management her. "Zusätzlich helfen Prozess- und IT-Standards, wie z.B: COBIT (Control Objectives for Information and Related Technology) und ITIL (Information Technology Infrastructure Library), die Compliance-Anforderungen zu erfüllen" (Schmelzer und Sesselmann, 2013, S.40).

4 Vorgehensmodell zur Integration von GRC in das Geschäftsprozessmanagement

"Prozessmanagement ist keine Disziplin der exakten Wissenschaften. Wenn Forschung und Entwicklung in diesem Kontext Erfolg haben sollen, müssen Forschungsergebnisse aufgrund von Beobachtungen, durch Experimente und auf Basis von Anwendungserfahrungen empirisch weiterführend untersucht und fortentwickelt werden." (Bayer und Kühn, 2013)

So wurde auch das Vorgehensmodell in dieser Arbeit basierend auf Praxiserfahrungen erarbeitet. Dies sind Erfahrungen über die in der wissenschaftlichen Literatur berichtet werden und die Praxiserfahrungen der Autorin.

Für die Entwicklung eines integrierten Vorgehensmodells wird das Vorgehensmodell des projektorientierten Geschäftsprozessmanagements nach NOVACESS sowie ein Vorgehensmodell zur Einführung des GRC-Managements nach Menzies (2009), ergänzt mit weiteren Elementen anderer Autoren, gewählt.

Man wird erkennen, dass es viele Berührungspunkte gibt bei Governance, Risikomanagement oder Compliance auf der einen Seite und den Tätigkeitsfelder des Prozessmanagements wie Prozessoptimierung, Prozessmodellierung oder kontinuierlicher Prozessverbesserung (KVP) auf der anderen Seite. Jedes GPM-System und jedes GRC-System sind maßgeschneiderte Management-Systeme. So viele verschiedene Unternehmenstypen es gibt, so unterschiedlich wird ihre Risikolage und ihre Geschäftsprozesse sein, so dass unterschiedliche Maßnahmen gewählt und angepasst angewendet werden müssen.

Es gibt einige kongruente Ziele des Prozess- und GRC-Management, die auf die gleiche Wertschöpfung im Unternehmen abzielen, dargestellt in Tabelle 2.

Ziele GRC-Management und Prozessmanagement
Effizienzsteigerung
Kundenzufriedenheit
Mitarbeiterzufriedenheit

Wettbewerbsvorteile
Qualitätssteigerung
Effektivität
Transparenz
Orientierung an Unternehmensstrategie

Tabelle 2: Gemeinsame Ziele von GRC und GPM

Zunächst soll jedoch das NOVACESS-Vorgehensmodell vorgestellt werden.

4.1 Vorgehensmodell GPM nach NOVACESS

Das in dieser Arbeit vorgestellte Einführungsmodell für GRC-GPM basiert für den Teil des Geschäftsprozessmanagements auf dem NOVACESS-Modell. Dies ist ein "Best-Practice-Ansatz für Projektorientiertes Prozessmanagement" (NOVACESS, 2015). Dieses Modell wurde auf Basis des stetigen Wandels in der Umwelt eines Unternehmens entwickelt und der daraus resultierenden Anforderung, dass auch die Prozesse in einem kontinuierlichen Verbesserungsprozess permanent daran angepasst werden müssen.

Das Modell nach NOVACESS ist ein phasenorientiertes Vorgehensmodell, beschrieben mit den dazugehörigen Methoden, Tools und Templates. Damit soll ein stetiges im Unternehmen fest verankertes Prozessmanagement implementiert werden (siehe Abbildung 12).

Abbildung 12: Vorgehensmodell Prozessprojekte nach Novacess (NOVACESS, 2015)

Kundenorientierung, Einbeziehung aller Stakeholder und Berücksichtigung der Unternehmensstrategie sind in dem Vorgehensmodell von NOVACESS von besonderer Bedeutung. Dabei werden folgende Phasen mit den dazugehörigen Tätigkeiten (Dräger und Rößler, 2012, S. 29 ff.) und Meilensteinen (Dräger und Rößler, 2012, S. 91) durchlaufen:

4.1.1 Strategie

Tätigkeiten

- Analyse der Ist-Situation (Status quo) der Organisation in Bezug auf Prozessmanagement und Sensibilität schaffen
- Reifegrad der Organisation und Prozesse auditieren
- Bestimmung Vision und Strategie
- Stärken-Schwächen ableiten
- Prozesslandkarte entwickeln und Kernprozesse identifizieren
- Festlegung angestrebter Kennzahlen
- Ziele und Anforderungsvorgaben für Prozessprojekt festlegen

Meilensteine

- Strategie ist Ressourcen- bzw. Marktorientiert festgelegt
- Kernprozesse sind identifiziert
- Fernziel/Vision ist festgelegt

4.1.2 Planung

Tätigkeiten

- Definition Projektziele abgeleitet aus strategischen Vorgaben
- Stakeholder-Analyse
- Zusammenstellung des Prozessteams
- Projektplanung (Vorgehen, Zeitplan, Meilensteine, Ressourcenplanung, Kostenabschätzung)

Meilensteine

- Projektauftrag ist vollständig beschrieben und abgenommen
- Projektorganisation benannt
- Vorgehensplan steht

4.1.3 Erfassung

Tätigkeiten

- Identifikation der relevanten Prozesse (strategische Vorgaben, Kunden-Produkt-Darstellung, Kundenwünsche)
- Erstellung Prozesslandkarte (Unterscheidung Kerngeschäftsprozesse und Unterstützungsprozesse)
- Aufnahme Ist-Prozess (Partizipative Methoden: Akzeptanz)
- Zuordnung korrespondierender Daten, Kennzahlen, Personen, Technologien und Validierung

Meilensteine

- Transparenter Ist-Zustand
- Relevante Daten sind erhoben
- Datenverantwortliche. -quellen sind dokumentiert

4.1.4 Analyse

Tätigkeiten

- Identifikation Schwachstellen/Handlungsfelder

- "Quick-Wins" umsetzen
- Schnittstellenanalyse (Prozessstrukturmatrix), Erfassung Informationsströme
- Ursachenanalyse
- Prozesskostenanalyse
- Anreizpräferenzen ermitteln
- Stand Wissensmanagement
- Ergebnisse kommunizieren

Meilensteine

- Kernursachen bzw. Treiber sind identifiziert
- Hauptangriffspunkte sind dokumentiert
- Basis für kreative Problemlösung ist geschaffen

4.1.5 Konzept

Tätigkeiten

- Optimierungsvorschläge/ neue Prozesse erarbeiten (Vision/Strategie beachten)
- Vorschläge auf Wirtschaftlichkeit prüfen (Aufwand-Nutzen-Matrix)
- Prozessoptimierung beschreiben
- Lösungsalternativen und Maßnahmen erfassen und Verantwortlichen mit Zeitangaben zuordnen (AKV)
- Prozesssteuerung entwickeln (Prozess-Scorecards)
- Qualifizierung Mitarbeiter (Kompetenzen schaffen)
- Change Management konzipieren
- Kommunikation konzipieren
- Wissensmanagement konzipieren

Meilensteine

- Optimierungsvarianten sind validiert
- Implementierungsplan steht
- Qualifizierungsmaßnahmen sind bestimmt

4.1.6 Implementierung

Tätigkeiten

- KVP-Konzept erarbeiten und umsetzen
- Laufende Prozessoptimierungen ermöglichen
- Pilotanwendungen
- Roll out planen und umsetzen
- Prozessdokumentation (Was ist zu tun, Wer verantwort, Wie wird verändert)
- Kommunikation durchführen
- Controlling installieren (Prozess-Scorecard gekoppelt mit Unternehmens-Scorecard)

- Anreizmanagement umsetzen
- Abschlussbericht zum Projekt und Erfassung Projektergebnisse in Wissensspeicher

Meilensteine

- Konzept ist umgesetzt
- Optimierte Prozesse sind vollständig implementiert, dokumentiert
- KVP und Prozesscontrolling sind installiert

4.1.7 Rollen

Dräger und Rößler (2012, S. 33) beschreiben folgende am Prozessprojekt beteiligte Rollen:

- Prozesskunden, -auftraggeber
- Projektleiter (Methoden, Instrumente und Werkzeuge Prozessmanagement; Change Manager)
- Prozessverantwortliche
- Prozessteam

4.1.8 Werkzeuge und Methoden

Es werden verschiedene Werkzeuge und Methoden zur Unterstützung des projektorientierten Geschäftsprozessmanagements in den jeweiligen Projektphasen vorgeschlagen (siehe Tabelle 3).

Die Werkzeuge und Methoden können je nach Anforderung und Voraussetzung passend ausgewählt und eingesetzt werden. Es werden also immer nur diejenigen eingesetzt, die auch benötigt werden.

Phase	**Werkzeug**
Strategie	Reifegradermittlung: Sensibilisierungsaudit Vision: Balanced Scorecard, Visionsworkshop Stärken-Schwächen-Analysen Kernprozesse, -kompetenzen: Geschäftsfeldmatrix Strategische Prozessprojekte Portfoliomanagement Prozessprojekte
Planung	Aufstellung Prozessteams: Stakeholder-Analyse Zieldefinitionen: SMART-Logik Projektmanagement

	Kommunikation: Rollen verteilen
Erfassung	Prozessidentifikation Erfassung Ist-Prozess: LIPOK,Brown-Paper, Wertstromdesign, PSM, Prozessfunktions-Diagramm Aufstellung Datenerhebungsplan
Analyse	Prozessanalyse: PSM, Wertstromdesign, Brown-Paper, Prozessfunktions-Diagramm, Werttreiber-Analyse Prozesskennzahlenanalysen: Pareto-Diagramm, statistische Auswertungen, Prozesskostenrechnung Organisationsanalysen
Konzept	Lösungen: Brainstorming, Prozess-Benchmarks Maßnahmenlisten Beschreibung Soll-Prozess Prozesssteuerung: Prozess-Scorecard, Prozesscontrolling Verantwortliche festlegen: AKV (Aufgaben-Kompetenz-Verantwortung)-Matrix Prozessdokumentation und -modellierung Lastenheft
Implementierung	KVP/Kaizen, A3-Bericht Prozessbeschreibung Prozessoptimierung Prozesscontrolling
Abschluss	Wissensspeicher Lessons Learned

Tabelle 3: Werkzeuge nach NOVACESS (2015) und Dräger und Rößler (2012)

4.2 Vorgehensmodell Einführung GRC-Management

Das hier vorgestellte Modell zur Einführung des GRC-Managements wurde in der Struktur von Menzies (2009) entwickelt. Die Autorin hat das Modell mit Erläuterungen zur Ablauflogik des strategischen GRC-Managements von Marekfia und Nissen (2009) und Elementen des ISO 19600 ergänzt. Dieses Modell in Kombination mit dem GPM-Einführungsmodell von NOVACESS ist Grundlage für das abgeleitete GRC-GPM Modell in Kapitel 4.3.

Im Folgenden werden die Tätigkeiten in den verschiedenen Phasen der erweiterten GRC-Umsetzungsmethodik für das GRC-Zielmodell nach Menzies (2009) dargestellt:

4.2.1 Analysephase

- Projektstart und Stakeholder-Analyse
    - Identifikation der Stakeholder und ihrer Anforderungen: Sichtung der identifizierten Anforderungen (Verträge, Gesetze, freiwillige Vorgaben) und Zuordnung zu Best Practices
- Erstellung und Pflege der unternehmensspezifischen Corporate Rule Base
    - "Instrument zur Aufnahme, Analyse und Überwachung aller externen und internen, gesetzlich vorgeschriebenen und freiwilligen Vorschriften und Vereinbarungen" (Menzies, 2009, S. 362) Dies ist ein Kernelement des Modells, in dem alle Stakeholderanforderungen erfasst werden. D.h. diese kann zusätzlich "bspw. Informationen zur strategischen Geschäftseinheit, zum Gültigkeitsbereich, zum Non-Compliance Risiko sowie eine Priorisierung der Anforderungen enthalten.
    - Identifikation von branchenunabhängigen Pflichtenkreisen (z.B. Arbeitssicherhei, Datenschutzrecht) und brachenbezogenen Pfichtenkreisen (z.B. Umweltrecht, Gentechnikrecht) (Wecker und van Laak, 2009)
- Aufnahme des unternehmensweiten GRC-Umfelds
    - Analyse von Organisation/ -Geschäftsprozessen hinsichtlich der Stakeholderanforderungen
    - Analyse der Prozesse hinsichtlich Risiko und Compliance-Anforderungen
    - Ableitung von GRC-Policies zur einheitlichen Umsetzung der Stakeholderanforderungen
    - Abgleich mit der Unternehmensstrategie
    - Betroffene IT-Systeme identifizieren
- Identifizierung von GRC-Potentialen
    - Analyse der Synergiepotentiale von GRC-Aktivitäten auf Grundlage der Auswertungen der Stakeholderanforderungen in der Corporate Rule Base zur Überwindung isolierter Umsetzungen der einzelnen GRC-Komponenten
- Identifizierung von GRC-Zielen
    - Risikoportfolio
- Projekt- und Change Management
- Analyse der gegebenen Anforderungen

4.2.2 Designphase

- Entwicklung des unternehmensspezifischen GRC-Zielmodells
- Entwicklung von Implementierungsstrategien

    - GRC-konformes Design der Geschäftsprozesse: "Die Anpassung der bestehenden Geschäftsprozesse kann hierbei die Prozesslogik selbst betreffen (z.B.: werden weitere Prozessschritte ergänzt), die aufbauorganisatorische Ausgestaltung (z.B. bei segregation of duties) aber auch die informationstechnische Ausgestaltung (z.B. Automatisierung, Prüfroutinen) betreffen" (Marekfia und Nissen, 2009, S. 13)
    - Risikomindernde Maßnahmen (z.B: Genehmigungsprozess für Änderungen der IT-Unterstützung, Änderungen am Prozess)
    - Compliance-Programm
- Trainings- und Schulungsmaßnahmen

4.2.3 Gestaltungsphase

- Entwicklung von GRC-bezogenen Komponenten der Organisation und Prozesse
- Entwicklung von GRC-bezogenen Systemen und Technologien
- Rollenzuweisung

4.2.4 Umsetzung und Kontinuität

- Implementierung GRC
- Unterstützung der Prozessbeteiligten gewinnen, Verantwortungen werden vergeben
- Kommunikation einschließlich Schulung
    - Kompetenzprüfung und -steigerung bei den Organisationsmitgliedern
    - Mitarbeiter verstehen ihre Rolle im Risiko-Management und Compliance
- Datengewinn für Controlling
- Dokumentation

4.2.5 Monitoring und Reporting

- Überwachung und Kontrolle des Systems (Effektivität und Effizienz)
    - Controlling: Prüfung auf Erfüllung der Anforderungen, Erreichung GRC-Ziele und Ausschöpfung Nutzenpotentiale
    - Kostenanalyse
- Berichterstattung
- Meldewesen implementieren und auswerten
    - Bei Non-Compliance-Vorfällen: Prüfung auf systemischen Fehler

4.2.6 Kontinuierliche Verbesserung

Verschiedene Einflussfaktoren können eine Anpassung des GRC-Managements erforderlich machen. Dazu zählen neue Geschäftsprozesse, neue Produkte oder Märkte, M&A-

Aktivitäten, neue IT-Systeme, neue Geschäftspartner und neue/veränderte GRC-Anforderungen (Menzies, 2009, S. 359). Dies macht eine kontinuierliche Verbesserung des GRC-Managements notwendig.

4.2.7 Rollen

Marekfia und Nissen (2009, S.9) leiten folgende Rollen ab, die für das GRC-Management notwendig sind:

- Das *GRC-Office* als Stabsstelle der Unternehmensleitung dient zur strategischen Ausrichtung und zentralen Koordination und setzt sich aus Geschäftsführung und tangierten Funktionsverantwortlichen (CIO, CFO, Leiter Recht usw.) zusammen.
- Das *GRC-Competence-Center* ist verantwortlich für die methodische und inhaltliche Integration einzelner Anforderungen und bindet Experten anderer Managementsysteme fallweise mit ein. Hier liegt auch die Verantwortung für eine laufende Aktualisierung und Kommunikation des GRC-Wissens in der Organisation.
- *GRC-Verantwortliche* sind GRC-Experten für einzelne, von GRC-Anforderungen betroffene Geschäftsprozesse und unterstützen die Prozessbeteiligten bei der Erfüllung der GRC-Anforderungen. Sie arbeiten eng mit den Prozessverantwortlichen zusammen oder haben diese Rolle selbst inne.

4.3 Vorgehensmodell integriertes GRC-GPM

Der Ansatz in dieser Arbeit zur integrierten Vorgehensweise bei der Einführung von GRC und GPM greift die wechselseitigen Beziehungen der einzelnen Teilelemente auf und zeichnet sich durch eine integrative und strategische Vorgehensweise aus. Unter Hervorhebung der integrativen Herangehensweise und der engen Verflechtung der einzelnen Komponenten wird der Ansatz hier als "integriertes GRC-GPM" bezeichnet.

Integration bedeutet dabei sowohl horizontal als auch vertikal. Horizontal heißt, dass GRC in die Prozesse integriert wird. Vertikale Integration bedeutet die Integration aller GRC und GPM Projekte und Initiativen zu einer strategischen unternehmensweiten Initiative. Außerdem ist der hier entwickelte Ansatz proaktiv. "Die proaktive Aktionsorientierung ist durch eine geplante, frühzeitige und unmittelbare Handlung gekennzeichnet und kann als die bewusste Gestaltung strategisch relevanter Tatbestände, um die Zukunft in einer für die Organisation günstige Richtung zu lenken konkretisiert werden" (Marekfia und Nissen, 2009).

Integriert werden das GPM-Vorgehensmodell von NOVACESS und das GRC-Vorgehensmodell nach Menzies (2009). Die einzelnen Phasen der Modelle sind hier zum besseren Überblick graphisch Dargestellt:

Abbildung 13: Phasen Vorgehensmodell GPM (NOVACESS, 2015) und GRC (Menzies, 2009)

Das Vorgehensmodell nach NOVACESS wurde für die Gegenüberstellung herangezogen, da dies bereits in mehreren Prozessprojekten in der Arbeitspraxis der Autorin eingesetzt wurde. Die GRC-Umsetzungsmethodik nach Menzies (2009) wurde gewählt, da diese nach Auffassung der Autorin durch die strukturierte Methodik gut in der Praxis einsetzbar ist und folglich zu einer hohen Akzeptanz bei den Projektbeteiligten führt. Außerdem ist es ebenfalls ein projektorientiertes Vorgehensmodell.

Die jeweiligen Tätigkeiten in den Phasen sind in Kapitel 4.1 (GPM) und 4.2 (GRC) dargestellt. Es ist zu erkennen, dass ähnliche Phasen durchlaufen werden (siehe Abbildung 13). Auch die durchzuführenden Tätigkeiten überschneiden sich teilweise (Synergieeffekte). Ansonsten können diese sich gegenseitig gewinnbringend ergänzen.

Die Phasen *Strategie* und *Planung* können zu einem großen Teil vom GPM übernommene werden, da das GRC-Modell erst mit der Analyse einsetzt, aber auch das GRC-Management von Strategie und Planung profitiert.

Die Phasen *Erfassung*, *Analyse*, *Konzept* und *Implementierung* des GPM werden mit den Phasen *Analyse, Design, Gestaltung* und *Umsetzung* des GRC zu folgenden neuen Phasen verbunden: *Erfassung, Analyse, Gestaltungskonzept* und *Umsetzung*. Die Phase *Monitoring* wird vom GRC übernommen. Dies ist auch ein Teil des projektorientierten Pro-

zessmanagements (z.B. in Form von KVP und Prozesscontrolling) und kann dort ebenfalls als eigene Phase angesehen werden, so dass ein Regelkreis entsteht. Einen Überblick über das entwickelte Modell bietet Abbildung 14.

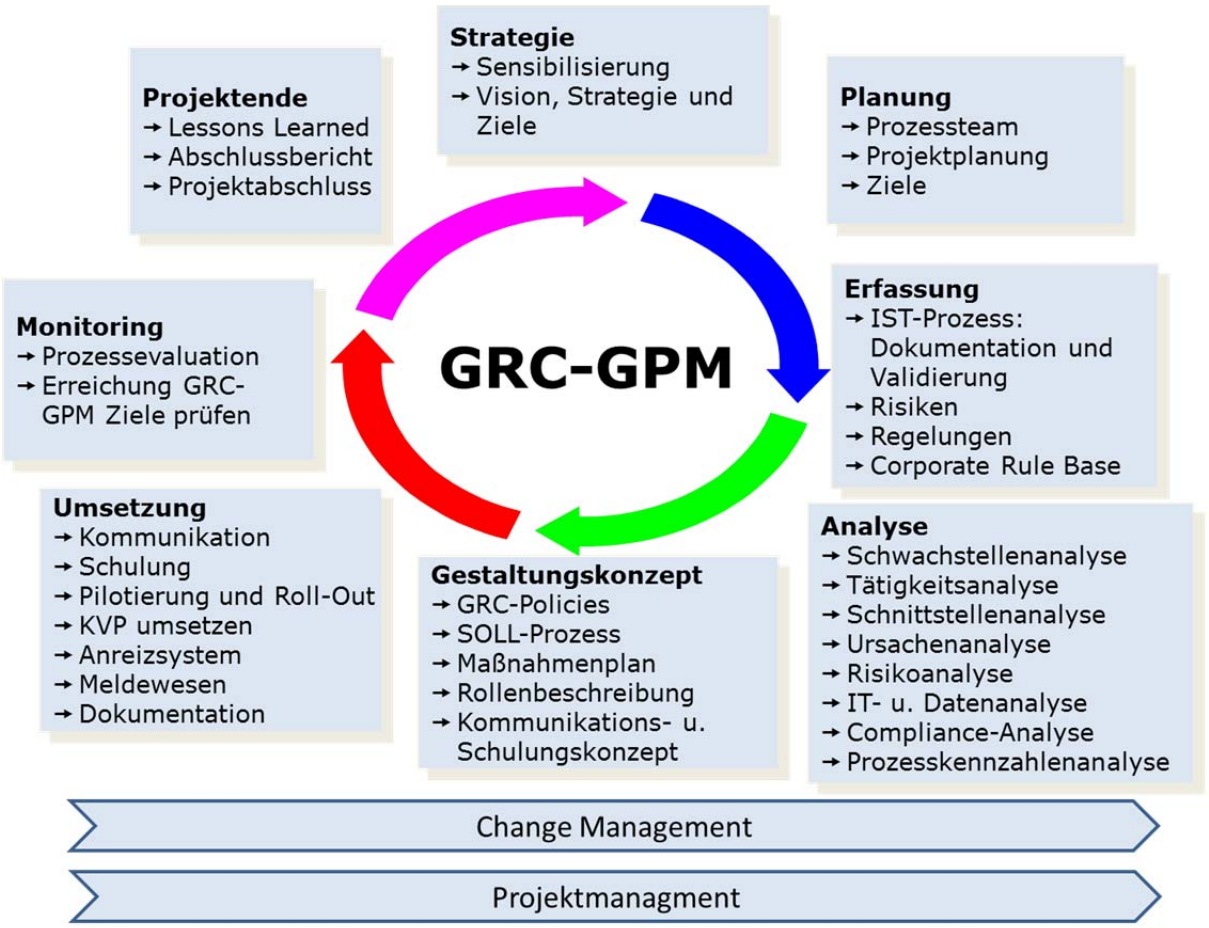


Abbildung 14: Vorgehensmodell GRC-GPM

Im Folgenden werden die einzelnen Phasen des Modells GRC-GPM detailliert dargestellt und erläutert. Empfohlene Werkzeuge und Methoden, die in den jeweiligen Schritten eingesetzt werden können sind *kursiv* gekennzeichnet, viele übernommen aus *Tabelle 3: Werkzeuge nach NOVACESS (2015) und Dräger und Rößler (2012). Die* detaillierte Erläuterung der Werkzeuge und Methoden ist nicht Teil dieser Arbeit und ist in der entsprechenden Fachliteratur zu finden (siehe Literaturverzeichnis). Die Tätigkeiten in den einzelnen Phasen sind zur besseren Lesbarkeit und der besseren Übersicht wegen stichpunktartig beschrieben.

Bei Anwendung des Modells sollte immer darauf geachtet werden, dass das angestrebte System auf das jeweilige Unternehmen angepasst wird (Größe, Branche, Risikopotential, etc.).

4.3.1 Strategie

Folgende Tätigkeiten sind in der ersten Phase, der "Strategiephase", durchzuführen:

Analyse der Ist-Situation (Status quo) der Organisation in Bezug auf Prozessmanagement und Sensibilität schaffen (*Portfoliomanagement Prozessprojekte*)

Reifegrad der Organisation und Prozesse auditieren (*Sensibilisierungsaudit*)

Vorläufige Prozesslandkarte entwickeln und Kernprozesse identifizieren (*Geschäftsfeld-matrix*)

- wo sind sie im Prozesshaus eingeordnet?
- wer ist für die Prozesse verantwortlich?
- sind bereits Schnittstellenprozesse bekannt?

Vision und Strategie definieren / Anlass zu Prozessneustrukturierung (*Balanced Score-card, Visionsworkshop, SWOT-Analyse*)

- wo soll die Reise hingehen?
- was möchte man eigentlich damit erreichen?
- Unterstützung der Führung einholen

Festlegung angestrebter Kennzahlen

Ziele und Anforderungsvorgaben für Prozessprojekt festlegen

- Welche Ziele verfolgt das GRC-GPM-System?
- Welche strategischen Zielsetzungen sollen durch das GRC-GPM-System unter-stützt werden?

Mit Hilfe der *Balanced Scorecard* wird die Strategie des Unternehmens umgesetzt. Sie kann dazu eingesetzt werden die Prozessziele zu definieren. Dadurch wird sichergestellt, dass die Prozessziele der Corporate Governance Strategie entsprechen.

4.3.2 Planung

In der zweiten Phase, der "Planungsphase", werden folgende Tätigkeiten zur Planung durchgeführt:

Prozessumfeld- und Stakeholder-Analyse (*Umfeldanalyse, Stakeholderanalyse, Stake-holderportfolio*)

- Identifikation aller prozessrelevanten Umfeldfaktoren, die zu berücksichtigen sind
- Identifikation der Stakeholder – wer profitiert von Veränderungen, wer wird beein-trächtigt, wer wirkt mit

- Identifikation der Stakeholder-Anforderungen: Sichtung der identifizierten Anforderungen (Verträge, Gesetze, freiwillige Vorgaben) und Zuordnung zu Best Practices

Prozessteam zusammenstellen und Rollen festlegen (*Rollenmatrix*)

- wer ist für was verantwortlich: klar benennen
- zusammen mit Prozessverantwortlichen festlegen
- vom Vorgesetzten absegnen lassen
- Zusammenstellung des Prozessteams unter Berücksichtigung der Stakeholder-Analyse
- GRC-Funktionen berücksichtigen und Teamfähigkeit sowie Erfahrung mit „ungewöhnlichen“ Projekten

Ziele zusammen mit Projektteam definieren und aus strategischen Vorgaben ableiten (*SMART-Logik*, *Zielhierarchie, Zieltabelle*)

- Zielhierarchie erstellen
- Ziele messbar formulieren

Projektplanung (*Projektmanagement-Methoden*: Vorgehen, Zeitplan, Meilensteine, Ressourcenplanung, Kostenabschätzung, etc.)

- Phasenplan: Grobgliederung des Projektes in Phasen und Meilensteine
- Projektsteckbrief: wichtige Eckdaten in einem Dokument
- Verteilung Steckbrief an Projektteam

4.3.3 Erfassung

Die dritte Phase, die "Erfassungsphase", umfasst folgende Tätigkeiten:

Prozesslandkarte erstellen (Unterscheidung Kerngeschäftsprozesse und Unterstützungsprozesse)

Prozessablauf der relevanten Prozesse (strategische Vorgaben, Kunden-Produkt-Darstellung, Kundenwünsche) im IST-Zustand erfassen (*Brown-Paper-Analyse, LIPOK, Wertstromdesign, PSM, Prozessfunktions-Diagramm*)

- Partizipative Methoden zur Prozess-Identifikation wählen, da dies die Akzeptanz fördert
- bereits bekannte Probleme kennzeichnen
- bekannte Verbesserungspotenziale aufnehmen
- Schnittstellen kennzeichnen
- Zuordnung korrespondierender Daten, Kennzahlen, Personen, Technologien und Validierung

Ggf. Expertengespräche führen

- d.h. mit einzelnen Beteiligten die jeweiligen Prozessschritte am Arbeitsplatz durchspielen/zeigen lassen

Dokumentieren aller Ergebnisse

Identifikation und Dokumentation von Risiken in Prozessen

Identifikation von Prozessen, die durch Regelungen betroffen sind

- Welche internen und externen Regelungen, welche Risiken und welche Governance Kodices haben Einfluss auf den Prozess?

Erstellung und Pflege der unternehmensspezifischen Corporate Rule Base (siehe Kapitel 4.2.1)

- Identifikation von branchenunabhängigen Regeln (z.B. Arbeitssicherheit, Datenschutzrecht) und brachenbezogenen Rgeln (z.B. Umweltrecht, Gentechnikrecht)

Review und Validierung der Ergebnisse dieser Phase durch das Projektteam

4.3.4 Analyse

Folgende Analysen werden in dieser vierten Phase, der "Analysephase" in Bezug auf die Prozesse vorgenommen:

Schnittstellenanalyse

- einzelne Schnittstellen tabellarisch auflisten
- beschreiben
- mit Projektbeteiligten bewerten
- Welche Risiken gibt es an den Schnittstellen? Welche Kontrollen sind notwendig, um den Risiken zu begegnen? (*Organigramme, Funktionsbeschreibungen, System Berechtigungskonzept, Prozess-/Risikoverantwortlicher*)
- Prozessstrukturmatrix
- Erfassung Informationsströme

Schwachstellenanalyse

- Schwachstellen in Prozessen

Tätigkeitsanalyse

- detaillierte Untersuchung der einzelnen Tätigkeitsschritte
- Welche Organisationseinheiten (bzw. Kompetenzen) und welche Mitarbeiter sollten an dem Prozess beteiligt sein?

Ursachenanalyse (*Ishikawa-Diagramm*)

- für Schwachstellen allgemein oder auch bei Schnittstellenproblemen
- Komplexe Zusammenhänge / Probleme detaillieren

Risikoanalyse (*Risikokontroll-Matrix, Risikoportfolio, Prozess-Fehlermöglichkeits- und Einflussanalyse, Szenarioanalyse* (Bayer und Kühn, 2013)*, Brainstorming*)

- Systemgestützte Risikoanalysen der relevanten Prozesse
- Risikokatalog definieren
- Identifizierung von Ereignissen oder Entwicklungen, die das Erreichen der definierten Ziele erschweren bzw. unmöglich machen.
- Risiken bewerten (*qualitative und quantitative Skalenmodelle*), wobei der durch die Corporate Governance festgelegte Risikoappetit des Unternehmens berücksichtigt wird
- Ergebnis der Bewertung für die Prozesse: kein Handlungsbedarf, Handlungsbedarf und akuter Handlungsbedarf (Bayer und Kühn, 2013)
- Stakeholderanforderungen und Strategie berücksichtigen

IT-Analyse (*Systemüberblick, Schnittstellenbeschreibungen*)

- Welche IT-Systeme sind im Rahmen des Prozesses im Einsatz und welche Schnittstellen gibt es?
- Welche Risiken sind damit verbunden?
- Welche Kontrollen sind notwendig, um den Risiken zu begegnen?

Datenanalyse (*Datenflussdiagramme, Datenmodelle*)

- Welche Daten werden in dem Prozess verarbeitet und wie sieht der Belegfluss bzw. Datenfluss im Prozess aus?
- Welche Risiken sind mit dem Datenfluss verbunden?
- Welche Kontrollen sind notwendig, um den Risiken zu begegnen?

Compliance-Analyse

- Compliance-relevante Prozesse analysieren (*Prozess-Compliance-Matrix*)
- identifizierte Stakeholder-Anforderungen und Strategie berücksichtigen

Identifizierung von GRC-Potentialen

- Analyse der Synergiepotentiale von GRC-Aktivitäten zur Überwindung isolierter Umsetzungen der einzelnen GRC-Komponenten
- Identifizierung von GRC-Zielen

Prozesskennzahlenanalysen (*Pareto-Diagramm, statistische Auswertungen, Prozesskostenrechnung*)

Sogenannte "Quick-Wins" direkt umsetzen

Anreizpräferenzen im Unternehmen ermitteln

Stand des Wissensmanagements ermitteln

Ergebnisse dieser Phase kommunizieren

4.3.5 Gestaltungskonzept

In der fünften Phase, der "Gestaltungskonzeptphase", werden die folgenden Tätigkeiten zur Konzipierung des Systems vorgenommen:

Entwicklung des unternehmensspezifischen GRC-Zielmodells (*Brainstorming, SMART-Logik*)

Ableitung von GRC-Richtlinien zur einheitlichen Umsetzung der Stakeholderanforderungen

- Wie werden die in der Analyse identifizierten Regelungen, Risiken und Governance Kodizes in den Prozessen einheitlich umgesetzt?

Optimierungsvorschläge/ neue Prozesse erarbeiten (Vision/Strategie beachten) und Sollprozesse definieren (*Brainstorming, Prozess-Benchmarks*)

- anhand Schwachstellen und Schnittstellenanalyse
- wie ist der Ablauf und wer soll was machen
- prüfen, dass die Kompetenzen der Mitarbeiter zu den Prozessanforderung passen
- Fragekatalog zur Schwachstellen-Analyse als Überprüfung
- Umsetzung der GRC-Anforderungen in den Prozessen durch entsprechende Prozessgestaltung (z.B. Einbau von Kontrollschritten, 4-Augen-Prinzip, IT-Prüfroutinen)
- An Aufgaben, Teilprozessen oder Ressourcen Risiken hinterlegen
- Kontrollen für Prozessrisiken definieren, die in der Analysephase mit Handlungsbedarf und akuter Handlungsbedarf bewertet wurden
- Risikomindernde Maßnahmen (z.B: Genehmigungsprozess für Änderungen der IT-Unterstützung, Änderungen am Prozess)
- Compliance-Scoping durchführen (*Prozess-Compliance-Matrix*): Bewertung der Prozesse in Bezug auf Compliance-Anforderungen möglichst normiert (Bayer und Kühn, 2013)
- Vorschläge auf Wirtschaftlichkeit prüfen (*Aufwand-Nutzen-Matrix*)

Maßnahmenplan festlegen (Erarbeitung im Projektteam, *Maßnahmenkatalog*)

- Gliederung in kurz,- mittel, und langfristig
- Verantwortlichkeiten zu Maßnahmen definieren (*AKV-Matrix*)
- Dokumentation der Maßnahmen

Rollenbeschreibung (*Rollenmatrix*)

- wer soll was machen
- prüfen, dass Kompetenzen der Mitarbeiter zu Prozessanforderung passen
- Kommunikation und Freigabe durch Vorgesetzte
- Prozessverantwortlichen und GRC-Verantwortlichen nochmals klar benennen

Kommunikationskonzept aufstellen (*Kommunikationsplan*)

- wer soll über was informiert werden
- mit welchen Medien

Schulungskonzept erstellen

- wo passen die Anforderungen nicht zu den Kompetenzen der Mitarbeiter und müssen vermittelt werden, welche Kompetenzen fehlen
- Schulungsunterlagen vorbereiten
- Zeitplan gemäß Kommunikationskonzept
- Zusätzlich auch Inhalte zu ethischen Entscheidungsfindungen und Verhaltensweisen basierend auf Werten und Prinzipien des Unternehmens, Integrität, Selbst-Bestimmung und Compliance

Prozesssteuerung entwickeln (*Prozess-Scorecards, Prozesscontrolling*)

Anreizsystem konzipieren

- Anreizsysteme, die regeltreuem Arbeiten nicht wiedersprechen (z.B. keine rein monetären Beurteilungen im Investmentbereich, keine Unterstützung des Anpassens an "landesübliche" aber illegale Verhaltensweisen, etc.).
- Leistungsbeurteilungen, die auch GRC- und Prozess-Können bewerten sowie Integrität und regeltreues Verhalten
- Arbeitsergebnisse, die durch regelwidrige Handlungen zustande kamen, werden nicht anerkannt

Meldewesen konzipieren

Kommunikation konzipieren

- Allgemeine Projektkommunikation
- Mitarbeiter verstehen ihre Rolle und Verantwortung in Prozessen und im Risiko-Management und Compliance

Wissensmanagement konzipieren und Zugriff auf GRC- und Prozess-Best-Practices und Richtlinien

Change Management konzipieren

Dräger und Rößler (2012) geben folgende Prinzipien für die Gestaltung von Prozessen vor, die in der Gestaltungskonzeptphase berücksichtigt werden sollten:

- So wenige Schnittstellen wie möglich,
- Mehrfacherfassung vermeiden
- Eindeutige Verantwortungen und Kompetenzen definieren
- Nur Prozesse definieren, die einen klaren Kundenbezug haben,
- Komplexität vermeiden

4.3.6 Umsetzung

In der "Umsetzungsphase", der sechsten Phase, sollten folgende Tätigkeiten abgearbeitet werden:

Verfahrensanweisung erstellen (*Verfahrensanweisung*)

Schulungskonzept umsetzen

- Kompetenzprüfung und -steigerung bei den Organisationsmitgliedern

Pilotphase und Roll-out planen

- welche „Versuchsgruppe“ und Termine
- Kommunikation an Pilotbeteiligte

Pilotierung durchführen

- Zeitrahmen setzen
- Minimalanzahl der Durchläufe festlegen

Kommunikation an alle (Projektteam, Prozessbeteiligte)

- Hintergrundinfos
- neue Verfahrensanweisung
- Schulungsvideo etc.
- Zeitplan der Umsetzung/Einführung
- wer ist Prozessverantwortlicher
- Unterstützung der Prozessbeteiligten gewinnen,
- Verantwortungen werden vergeben

Roll-out durchführen

- Feedbackgespräche 360 °C: Stichprobenartig von allen Prozessbeteiligten Feedback einholen oder als Workshop organisieren

- Wünsche/Anregungen zu neuen Prozess sammeln, nicht auf Zuruf sofort einbinden/umsetzen (*Weiterentwicklungsplan* aufstellen und zusammen mit Prozessverantwortlichen festlegen, was ggf. angepasst werden muss)
- Im Risikoportfolio definierte Kontrollen in der Organisation nachhaltig verankern (Bayer und Kühn, 2013):
    - als IT-Kontrollen in der bzw. in den betroffenen Applikationen,
    - als Arbeitsanweisung für die Mitarbeiter,
    - als Kontrollen im Ablauf des betroffenen Prozesses,
    - als Kontrolle in der Aufbauorganisation, die z. B. zur Funktionstrennung dient,
    - als Kontrolle in der Infrastruktur, die IT-Berechtigungen oder Zutrittsbeschränkungen reguliert.

KVP-Konzept erarbeiten und umsetzen (*Kaizen*)

- Laufende Prozessoptimierungen ermöglichen
- Controlling installieren (Prozess-Scorecard gekoppelt mit Unternehmens-Scorecard) und Ergebnisse aus Prozesskontrollen mit einbeziehen
- Prozess zur kontinuierlichen Integration neuer gesetzlicher oder interner Regularien in die Prozesse definieren

Prozessdokumentation (Was ist zu tun, Wer verantwortet, Wie wird verändert)

- Prozessmodelle werden Bestandteil des Risikomanagementhandbuchs
- Einordnung von Regularien und Risiken in die Prozesslandkarte zur besseren Übersicht und Transparenz
- Regelungen, Anweisungen, Verordnungen, etc. werden in den Prozessbeschreibungen schriftlich fixiert

Anreizmanagement umsetzen

Meldewesen implementieren

Entwicklung von GRC-GPM-bezogenen Systemen und Technologien

Change Management beachten

Wissensmanagement umsetzen

4.3.7 Monitoring

Grundlage des Monitorings ist der Geschäftsprozess bzw. sein Modell. "Erfahrungen insbesondere bei der Neukonzeption von Geschäftsprozessen zeigen, dass in der Regel nicht a priori sichergestellt werden kann, dass der entworfene Prozess auch tatsächlich den aus Kunden- und Prozesseignersicht gewünschten Output produziert" (Schmidt,

2009, S.19). Daher ist es notwendig ein ständiges Prozesscontrolling durchzuführen, was zu einem GRC-GPM-Zyklus führt, wie in Abbildung 14 dargestellt.

Um dem Anspruch einer kontinuierlichen Verbesserung zu genügen, führt eine wiederholte Durchführung des GRC-GPM-Zyklus zu einer nachhaltigen Verankerung im Unternehmen und kann iterativ evaluiert und verbessert werden.

Die Projekterfahrung zeigt, dass in den meisten Fällen nach einem dreimaligen Durchlauf das System nachhaltig verankert ist, da sich dadurch der Lerneffekt der Mitarbeiter eingestellt hat und das GRC-GPM als fester Bestandteil des Unternehmens angesehen wird. Dabei ist es wichtig den Nutzen des integrativen Systems den Mitarbeitern ständig bewusst zu machen, da diese die wesentliche Quellen für Verbesserungsvorschläge sind (Bayer und Kühn, 2013, S. 339). So sollten folgende Tätigkeiten in dieser Phase durchgeführt werden:

Iterationsintervall zur Prozessbetrachtung festlegen und Kennzahlen definieren um Prozesse zu messen

- Prozessevaluation: Schwachstellen/Risiken für Erfassung und Analyse festhalten
- Risikosteuerung: Anhand von Schwachstellen/Risiken Vorgaben für Prozessdesign machen

Erreichung GRC-GPM-Ziele

- Sind Governance, Risiko-Management und Compliance-Management integriert, holistisch und organisations-weit in den Prozessen implementiert?
- Sind die Prozess-Ziele von den Unternehmenszielen abgeleitet?
- Wird ethisches Verhalten gefördert bzw. nicht-ethischem Verhalten vorgebeugt?
- Entwickelt sich das Risikoportfolio in die gewünschte Richtung?

Überwachung und Kontrolle des Systems auf Effektivität und Effizienz

- Ergebnisse aus Prozess-Controlling auswerten
- Prüfung auf Erfüllung der Anforderungen und Ausschöpfung Nutzenpotentiale
- Kostenanalyse

Berichterstattung

- z.B. Heat *Maps* zur Darstellung der Prozess-Compliance und Risiko-Bewertung (Bayer und Kühen, 2013)
- *Process Passorts, Process Portfolios* (Bayer und Kühen, 2013)

Meldewesen auswerten

- Bei Non-Compliance-Vorfällen: Prüfung auf systemischen Fehler

4.3.8 Projektabschluss

Beim Projektabschluss sollten folgende Tätigkeiten durchgeführt werden:

Lessons Learned und Abschlussbericht erstellen

Prozess an Prozessverantwortlichen übergeben (Weiterentwicklungsplan übergeben)

Projektabschlusssitzung mit Projektteam

Abschlussbericht zum Projekt und Erfassung Projektergebnisse in *Wissensspeicher*

4.3.9 Rollen

Folgende Rollen sind an dem Einführungsprojekt zum strategischen GRC-GPM beteiligt, wobei die Prozessverantwortlichen, GRC-Verantwortlichen, das GRC-Office und das GRC-Competence-Center dauerhaft implementiert werden sollten:

- Prozesskunden, -auftraggeber
- Projektleiter (Methoden, Instrumente und Werkzeuge Prozessmanagement und GRC; Change Manager)
- Prozessverantwortliche und GRC-Verantwortliche (arbeiten eng mit den Prozessverantwortlichen zusammen oder haben diese Rolle selbst inne)
- Prozessteam
- GRC-Office (Geschäftsführung und tangierte Funktionsverantwortliche (CIO, CFO, Leiter Recht usw.))
- GRC-Competence-Center (Risikomanager, Compliance-Manager)

4.3.10 Begleitend

Change Management

Bei jedem Projekt in einer Organisation, das solche wesentlichen Änderungen mit sich bringt, sollten Maßnahmen zur Mitarbeitersensibilisierung und Akzeptanzsicherung umgesetzt werden.

Hierbei unterstützt das Change Management. Nicht nur bei der Einführung des Geschäftsprozessmanagements, sondern auch bei der Ausführung werden ständig Veränderungen realisiert. Um dies zu begleiten, ist das Change Management unentbehrlich (Schmelzer und Sesselmann, 2013).

Die Unternehmensleitung muss das neue System aktiv unterstützen, den GRC-GPM Funktionen entsprechende Unabhängigkeit und Zuständigkeiten gewähren und das System regelmäßig überprüfen. Daher ziehen sich die verschiedenen Aktivitäten des Change

Management durch jede Phase des Projekts und sollten nach Ansicht der Autorin immer als von Anfang bis Ende kontinuierlich begleitende Maßnahme betrachtet werden.

Projektmanagement

Auch die einzelnen Aktivitäten des Projektmanagement finden sich in jeder Phase des GRC-GPM-Projekts wieder. Es ist wichtig bei Nutzung des Modells, auch das Projektmanagement als ständig begleitende Maßnahme konsequent und gründlich durchzuführen. Nur so kann GRC-GPM effizient und effektiv eingeführt werden, da das Projekt Management unterstützt, die richtigen Maßnahmen von den passenden Personen zur richtigen Zeit in der passenden Reihenfolge durchzuführen.

5 Bedeutung des Modells für GPM und GRC

Der Lösungsbeitrag des Modells zur Überwindung aktueller Herausforderungen in GPM und GRC wird hier von der Autorin auf Grundlage von qualitativen Interviews mit Experten (siehe Anlage) und diversen Erfahrungsberichten und Studien aus der wissenschaftlichen Literatur hergeleitet.

"Geschäftsprozessmanagement befähigt Organisationen, flexibel auf Veränderungen zu reagieren und erforderliche Anpassungen vorzunehmen. Es leistet wichtige Beiträge zur Steigerung der Organisationskompetenz und -effizienz." (Schmelzer und Sesselmann, 2013, S. 2) Dies ist eine in der wissenschaftlichen Literatur einheitliche Meinung. Allerdings fällt es vielen Unternehmen schwer, diesen Ratschlag umzusetzen.

Eine Studie von PwC (2011) stellte fest, dass sich Führungskräfte dahin gehend einig sind: "Unternehmen können in den kommenden 10 Jahren im Wettbewerb nur dann bestehen, wenn sie kontinuierlich an der Verbesserung ihrer Geschäftsprozesse arbeiten.“ Aber: "Die Analyse auf der Basis der von uns durchgeführten Umfrage deckt jedoch auf, dass die Umsetzung des Geschäftsprozessmanagements bei Weitem nicht so gezielt und umfassend stattfindet, wie es mit den zur Verfügung stehenden Methoden und analytischen IT-Systemen möglich wäre."

Organisationen weltweit versuchen durch das Geschäftsprozessmanagement effektiver und effizienter zu arbeiten. Effektiv zu handeln, bedeutet die richtigen Dinge zu tun. D.h. es ist von großer Bedeutung Strategie und Ziele zu formulieren und die Aktivitäten im Unternehmen konsequent daran auszurichten. Laut Schmelzer und Sesselmann (2013, S. 3) haben viele Unternehmen ein "Defizit, was ihre Effektivität anbelangt. Beispiele sind: kein überzeugendes Leitbild, unklare strategische Ziele, mangelhafte Kenntnis von Erfolgsfaktoren und Erfolgspotenzialen, unklare Marktziele, unzureichende Kenntnis der Kundenprobleme, -bedürfnisse, -anforderungen und -erwartungen, unklare Prozess- und Produktziele."

In der Studie "Business Process Centers of Excellence Survey" (BPTrends Process Centers, 2012) wurde festgestellt, dass nur 31% der Unternehmen GPM strategisch ausgerichtet haben. Laut der Studie "The State of Business Process Management" (BPTrends BPM, 2012) geben 37% der Befragten an, dass das oberste Management nicht am Prozessmanagement interessiert ist.

Ein funktionierendes und integriertes GRC-Management führt zu guten und umfassenden Zielen und der entsprechender Strategie. Daran kann sich dann das Prozessmanagement ausrichten und in die "richtige Richtung " arbeiten. Sind Ziele und Strategie im Unternehmen nicht gesetzt oder nicht durchdacht, kann auch das Prozessmanagement nicht effizient funktionieren. Dabei hilft die integrierte Umsetzung von GRC und GPM. Es sorgt

dafür, dass die Ziele, Strategie und Richtlinien der Unternehmung fester Bestandteil des GPM sind.

Auch bei der Effizienz (die Dinge richtig tun) haben viele Organisationen Defizite. "Besonders stark verbreitet sind Effizienzprobleme in Prozessen. Eine niedrige Prozesseffizienz wirkt sich nicht nur negativ auf die Produktivität aus, sondern belastet über unzureichende Produktqualität, geringe Termintreue und lange Durchlaufzeiten zusätzlich die Kundenzufriedenheit und damit den Umsatz." (Schmelzer und Sesselmann, 2013, S.3) Das integrierte GRC-Management ist ein nützlicher Faktor, um die Prozesseffizienz zu steigern.

Die Studie "The State of Business Process Management" (BPTrends BPM, 2012) hat weiterhin gezeigt, dass auch in der bereichsübergreifenden Koordination von Abläufen noch große Verbesserungspotenziale bestehen. Dies haben auch die Interview-Partner der Autorin bestätigt. In deren Arbeitsalltag ist das funktionale Denken vorherrschend. Dadurch entstehen nach Ansicht der Autorin Hindernisse bei der Schnittstellenabstimmung, da verschiedene Akteure mit unterschiedlichen Sichtweisen und "Inseldenken" mit eingebunden werden müssen und somit die Umsetzung des GPM stark erschwert wird. Auch dabei kann das integrierte GRC im GPM unterstützen. Den Vorgesetzten in den Fachbereichen helfen die Prozessdokumente, ihre gesetzlich und betriebsintern geforderten Führungs- und Kontrollaufgaben wahr zu nehmen. Den Mitarbeitern geben Prozessmodelle Sicherheit bezüglicher ihrer eigenen Aufgaben und Entscheidungsmöglichkeiten.

5.1 Prozessoptimierung

Sollen Prozesse hinsichtlich Effektivität und Effizienz optimiert werden so können durch das integrierte GRC-GPM die analysierten Risiken in die Priorisierung der möglichen Optimierungsprojekte einfließen. Neben weiteren Kriterien, wie z. B. der strategischen Relevanz, dem Ergebnis der Kosten-Nutzen-Analyse oder der Größe des jeweiligen Handlungsbedarfs, können jene Optimierungsprojekte festgelegt werden, welche hinsichtlich der Risikobewertung dringend durchzuführen sind (Bayer und Kühn, 2013).

Eine Studie von PwC (2011) stellte fest: "Compliance und Governance: Weitere Ziele stehen in engem Zusammenhang mit Gesetzen, Richtlinien und Normen. Das Geschäftsprozessmanagement hat sicherzustellen, dass die Abläufe eines Prozesses transparent werden, um beispielsweise „Compliance-Vorschriften“ einzuhalten und „Umwelt- und Sicherheitsauflagen“ erfüllen zu können oder die „Sicherstellung der Nachvollziehbarkeit und Vertrauenswürdigkeit für die Buchhaltung“ zu gewährleisten."

„Durch die Einbindung von Compliance-Frameworks in die Prozessorganisation wird einerseits zu einer risikoorientierten Steuerung der Unternehmensabläufe beigetragen und andererseits auch Input für die kontinuierliche Prozessverbesserung geliefert“ (Bayer und Kühn, 2013, S. 116). So kann beim isolierten GPM die Gefahr bestehen, dass Prozesse durch neue Regularien illegal werden. Durch das integrierte GRC-GPM werden die neuen Regularien direkt an den Prozessen umgesetzt.

5.2 Risikomanagement

Die operationelle Risiken (technische, menschliche und organisatorische) sind im Prozessmanagement von großer Bedeutung. Dabei können Risiken auftreten, die aus fehlerhaften oder instabilen IT-Systemen, aus Unachtsamkeit oder dolosen Handlungen oder aus unklaren Entscheidungsberechtigungen, fehlenden 4-Augenprinzipien oder fehlenden Prozessdokumentationen stammen.

Das Risikomanagement profitiert erheblich davon, bereits beim anfänglichen Prozessdesign und danach bei der ständigen Prozessoptimierung Risiken und Kontrollen in den Prozessablauf zu integrieren und dort für alle Beteiligten transparent zu dokumentieren. Dabei werden direkt im Prozess an Aufgaben, Teilprozessen oder Ressourcen Risiken und Kontrollen hinterlegt (durch eine geeignete Prozessnotation und passende Risikosymbole) oder übergreifende Risiken für den gesamten Prozess als Input mit entsprechenden Kontrollen vermerkt.

Derzeit ist es laut Aussage der Interview-Partner noch häufig so, dass von Prozessmanagern auf der einen Seite ausführliche Prozessdokumentation erstellt werden und auf der anderen Seite Führungskräfte oder Risikoexperten die für ihren Bereich relevanten Daten in einer Risiko-Kontroll-Matrix führen. Dies ist eine Tabellenkalkulation in dem neben den Risiken und Kontrollen auch weitere Informationen wie ökonomische Auswirkungen des Risikos oder eine Beschreibung der Kontrolle übersichtlich dargestellt werden. Durch das integrierte GRC-GPM Modell werden die operationellen Risiken mit den dazugehörigen Kontrollen bereits in der Prozessmodellierung berücksichtigt. Daraus ergeben sich nach Ansicht der Autorin zum Teil erhebliche Einsparpotenziale für die Planung und Überwachung der Risiken und Kontrollen.

5.3 Compliance

Bei den wirtschaftskriminellen Skandalen in der Vergangenheit (wie z. B. Volkswagen, Enron oder Siemens) haben die betroffenen Firmen im Vorfeld einen Code of Ethics, einen Code of Conduct, Compliance Officer, vielleicht sogar eine Compliance Hotline und vieles andere eingesetzt und trotzdem ist es zu den Vorfällen gekommen (Wieland, 2008). Diese Compliance-Programme haben ihr Ziel, nämlich präventiv zu schützen, nicht erfüllt.

Nach Aussage der Interview-Partner laufen viele Firmen heute Gefahr ihre Compliance-Systeme mit den falschen Schwerpunkten anzulegen und diese nicht konsequent in alle Bereiche des Unternehmens auszuweiten. So wird beispielsweise sehr genau festgelegt, welchen Wert Geschenke an Geschäftspartner haben dürfen oder in welchem Wert Geschenke empfangen werden dürfen oder wie Reise- und Spesenabrechnungen zu handhaben sind. Das große Ganze kommt aber häufig zu kurz. Für die schwerwiegenden Themen, die sich direkt auf das Kerngeschäft auswirken fehlen häufig diejenigen, die sich verantwortlich fühlen Risiken zu kommunizieren oder Regelungen zu erstellen. Für Themen rund um die gesellschaftliche Verantwortung, wie z.B. Umweltschutz oder Produkti-

onsbedingungen fehlen häufig eindeutige Regeln und die Compliance Beauftragten sind weit weg vom Tagesgeschäft. Nach Ansicht der Autorin kann das in dieser Arbeit vorgestellt integrieret Vorgehen dazu beitragen, dass Compliance in alle Winkel einer Organisation getragen wird, indem es Bestandteil jedes Prozesses ist. Außerdem werden für jeden Prozess Prozess- und GRC-Verantwortliche implementiert, die sich dafür verantwortlich fühlen die nötigen Regelungen für ihre Prozesse einzuführen.

Bestimmte strukturelle Mechanismen können individuelles Fehlverhalten auslösen und stabilisieren und damit zu einem unkalkulierbaren Risiko machen (Wieland, 2008). Strukturelle Anreize in Geschäftsprozesse können individuelles Fehlverhalten auslösen. Um dem entgegen zu wirken, werden Prozesse geschaffen, bei denen sich wirtschaftlicher Erfolg und regelkonformes Verhalten gegenseitig als Voraussetzung haben und nicht das jeweils andere ausschließen. Sowohl die Transparenz, die durch die implementierten Prozesse geschaffen wird, trägt dazu bei, diese strukturellen Anreize wirksam auszumerzen, als auch die gezielte und geplante Analyse und Implementierung von Anreizsystemen, die regeltreuem Arbeiten nicht wiedersprechen (wie das z.B. der Fall sein kann bei rein monetären Beurteilungen im Investmentbereich oder der Unterstützung des Anpassens an "landesüblichen" Verhaltensweisen).

Die Umsetzung des Compliance Management direkt an den Geschäftsprozessen verhilft auch zu einer größeren Flexibilität. Das GPM wird eingesetzt, um schnell und flexibel auf Änderungen am Markt einzugehen. So kann dieses auch eingesetzt werden, um schnell und flexibel auf veränderte Gesetzeslagen zu reagieren. "Unternehmen, die sich frühzeitig auf neue Regeln und Standards einstellen und vorbereiten, haben gegenüber ihren Wettbewerbern Vorteile, weil deren Implementierung erfahrungsgemäß wirksamer und auch kostengünstiger ist, je eher mit der Umsetzung begonnen wir" (Menzies, 2009, S. 3)

Externe wie interne Compliance-Stakeholder wollen immer öfter Einblick in die Prozessabläufe bekommen. Dabei werden bspw. Fragen gestellt, wie (Bayer und Kühn, 2013, S. 116):

- An welcher Stelle in welchen Prozessen wird die Compliance-Anforderung X berücksichtigt?
- Wie lautet die Einschätzung eines Prozessverantwortlichen in Bezug auf den Erfüllungsgrad der Compliance-Anforderung Y?
- Wie ist der durchschnittliche Compliance-Grad für den Prozessbereich Z jetzt und welcher Wert soll in Zukunft erreicht werden?

Auch dabei unterstützt die integrierte Vorgehensweise. Durch die im Modell vorgesehene Integration in die Prozesse, die Dokumentation an den Prozessen und die Implementierung von Prozess- und GRC-Verantwortlichen können diese Fragen ohne großen Aufwand beantwortet werden. So haben auch die Interview-Partner angegeben, dass Compliance-Dokumente (Richtlinien) in die Prozessdokumentation integriert wurden.

5.4 Governance

Nach Aussage der Interview-Partner gibt es in einem Unternehmen immer Aktivitäten zur Corporate Governance, ob diese Aktivitäten nun geplant angegangen werden oder nicht. Ungeplante und unkoordinierte Governance Aktivitäten können jedoch willkürliche Zielsetzungen und Entscheidungen, politische Machtkämpfe und verschwendete Ressourcen aus wirren und miteinander konkurrierenden Anstrengungen zur Folge haben. Wird aber dagegen geplant und strukturiert vorgegangen, wie in dem hier vorgestellten Modell, so kann dieser Problematik gezielt entgegengewirkt werden.

Auch die Studie von PwC (2011) hat ergeben: "Das Geschäftsprozessmanagement muss als Führungsfunktion im Unternehmen organisatorisch verankert und mit den notwendigen Entscheidungskompetenzen ausgestattet sein." Ist dies der Fall, so ist sichergestellt, dass auch die Governance-Prozesse strukturiert und zielgerichtet organisiert sind.

5.5 Interne Revision

Die Interne Revision profitiert ebenfalls von einem integrierten Vorgehen und kann zum GPM gewinnbringend beitragen. So schreiben beispielsweise Frigo und Anderson (2009 S. 34): „Internal auditing is often involved in these initiatives, given its role as a critical grc function. grc initiatives can provide internal auditors with numerous opportunities to enhance audit processes and knowledge activities.“

Durch die dokumentierten Prozesse wird den Überwachungsorganen, wie Interne Revision, Risikomanager oder Compliance-Officer, die Arbeit erleichtert, weil sie so einfacher ihrer Prüfungs- und Beratungstätigkeit nachkommen können. Um gegebenes Fehlverhalten innerhalb des Prozessablaufs feststellen zu können, muss klar sein, wie der richtige Prozess aussieht. Durch die Dokumentation des Ablaufes, ist es für Dritte leichter nachvollziehbar, ob die Prozessbeteiligten ihre dort festgelegten Aufgaben regeltreu erfüllen. Je einheitlicher und durchgängiger eine risikoorientierte Prozessdokumentation im Unternehmen gelebt wird, desto leichter fällt den Prüfern die Arbeit. So gaben die Interview-Partner an, dass Revisoren, Wirtschaftsprüfer und sonstige Kontrollorgane bei ihren Prüfungen zunehmend klare Anforderungen an eine ordentliche Prozessbeschreibung stellen und die Arbeit der Prüfer durch Einführung von einheitlichen Prozessdokumentationen wesentlich erleichtert wurde.

Durch die interne Revision wird im Rahmen von umfangreichen Systemprüfungen oder durch stichprobenartige Querschnittsprüfungen geprüft, ob die Prozessregelungen und das Risikomanagement umgesetzt wurden und ob diese zielführend sind. Dabei können auch Prozessrisiken wirkungsvoll identifiziert werden, Schwächen in den Kontrollen aufgedeckt werden und Ideen zur Prozessoptimierung erarbeitet werden.

5.6 GRC

Bei den Interviews wurde festgestellt, dass es erhebliche Nachteile gibt, wenn die einzelnen GRC-Disziplinen getrennt voneinander betrachtet werden. Führt man Governance, Risiko-Management und Compliance getrennt voneinander und ohne Integration in das Prozessmanagement ein, so ist das Ergebnis meist ein Durcheinander von Kontrollen und Praktiken, die in Funktionalen oder geographisch getrennten Silos durch etliche isolierte Aktivitäten umgesetzt werden. Dies führt zu einer sehr hohen Komplexität und Redundanz des Systems, das große Lücken in Regelungen und Risikobetrachtungen offen lässt. Das ist sehr teuer und führt offensichtlich nicht zu einem erwünschten Ergebnis. So kann es dann z.B. vorkommen, dass eine Führungskraft Anfragen von Compliance, internen Auditoren, Rechtsberatern oder Risikomanagern erhält, die letztendlich die gleiche Information benötigen, wenn auch vielleicht in leicht unterschiedlichen Ausführungen. Gleichzeitig gibt es keinen ausreichenden Überblick über die Risiken.

In einer Auftragsstudie hat PwC (2004) herausgefunden, dass viele Organisationen keine signifikanten Echtzeit GRC-Event, Prozess und Report-Möglichkeiten haben. Fast ein Drittel der Industrie-Teilnehmer berichteten, dass sie noch weit entfernt von der Umsetzung von Echtzeit-GRC-Reporten sind. Dies kann mit Hilfe von integriertem GRC-GPM und der entsprechenden IT-Unterstützung schneller erreicht werden.

Die Studie von NTT DATA (2013) hat ergeben, dass sich eine Zusammenarbeit von Compliance mit dem Risikomanagement und dem Internen Kontrollsystem nur in einem Viertel der Unternehmen findet. Die einzelnen GRC-Disziplinen greifen aber ineinander und basieren auf den gleichen Prozessen, Mitarbeitern und Daten im Unternehmen. Mit dem integrierten Ansatz zu GRC und GPM kann man dies effizient realisieren und bekommt Zugang zu verlässlichen Informationen, die man braucht um sichere Entscheidungen zu treffen und Risiken effektiv zu steuern. Dies kann zu Kostensenkungen, verbesserten Risiko- und Compliance-Management und schnellerem und einfacherem Zugang zu wichtigen Informationen führen.

Wenn Governance in die Prozesse eines Unternehmens integriert wird, dann wird das Risiko minimiert, dass Governance, Risiko und Compliance isolierte "Elfenbeinturm-Aktivitäten" bleiben (Schmelzer und Sesselmann, 2013). Bei der Integration von GRC in das Prozessmanagement ist insgesamt weniger organisatorischer Aufwand für das GRC erforderlich. Durchführung, Kontrolle und Verantwortung der einzelnen Maßnahmen werden im Rahmen des Geschäftsprozessmanagements geregelt. Prozess- und GRC-Verantwortung kann auf einer Person gebündelt werden.

Eine Kultur der Prozessvisualisierung begünstigt auch die Berücksichtigung von Risikofaktoren oder Compliance-Regeln im Arbeitsablauf, da diese einfach in den Prozessen mit speziellen Notationen kenntlich gemacht werden können. Durch diese Transparenz von Regelungen, "ist es möglich, Änderungen von Compliance-Vorschriften und -Richtlinien schnell und effizient zu berücksichtigen" (Schmelzer und Sesselmann, 2013, S. 40).

Im Rahmen von Reformbemühungen der Gesetzgebung zu Compliance Systemen schlägt das Deutsche Institut für Compliance sogar vor, dass es Strafmilderungen gibt, wenn ein Unternehmen ein umfangreiches Compliance-System implementiert hat. Dieses sollte dann auch Prozess- und Ablaufbeschreibungen enthalten (Holz, 2015). Wenn Compliance, Risiko-Management und Governance tief in die Prozesse integriert sind, dann kann dies als ein Indikator für eine ernsthafte Bemühung, ein umfangreiches Compliance-System implementiert zu haben, angesehen werden. Dies führt dazu, dass im Ernstfall die Rechtsprechung milder ausfallen kann.

6 Schwierigkeiten, Grenzen und Voraussetzungen

Auch die Evaluierung des Modells in diesem Kapitel basiert auf qualitativen Interviews mit Experten (siehe Anlage) und diversen Erfahrungsberichten und Studien aus der wissenschaftlichen Literatur. Eine wesentliche Grenze des Modells ist nach Ansicht der Autorin derzeit die nicht ausreichende praktische Erprobung des Modells und Evaluierung der Ergebnisse. Dies geht über den Umfang dieser Arbeit hinaus und sollte in darauf aufbauenden Arbeiten untersucht werden.

6.1 Voraussetzungen

Es muss in jeder Organisation evaluiert werden, welche Vorgehensweise dort die richte zur Umsetzung von GRC-GPM ist. Wie auch bei der isolierten Einführung von GPM, sollte hier überlegt werden, ob eine umfangreiche unternehmensweite Umsetzung gewählt wird oder ein schrittweises Vorgehen, in dem Bereich für Bereich nacheinander verändert wird. Nach Ansicht der Autorin kann dies nicht pauschal für jede Organisation empfohlen werden, da es sehr stark auf die örtlichen Gegebenheiten ankommt.

Die Interview-Partner sprachen sich in ihren Bereichen für ein schrittweises Vorgehen aus. Auch Bayer und Kühn (2013, S.310) empfehlen ein schrittweises Vorgehen: "Um dies zu schaffen, ist ein Big Bang-Vorgehen nur selten sinnvoll – vielmehr sollten die Schaffung von Management-Awareness sowie das Vorantreiben der Integration auf Basis selektiver, nach Optimierungspotenzialen priorisierter Bereiche im Fokus stehen. Auf diese Weise können einerseits Quick Wins erzielt werden. Andererseits hat die Organisation ausreichend Zeit, sich an die Änderungen anzupassen. Eine parallel ablaufende, saubere IT-Umsetzung fördert dazu die Nutzbarkeit und sukzessive die Nutzung der Steuerungselemente (Ziele, KPI, Maßnahmen) auf allen Ebenen."

Prozessorganisation (PwC, 2011)

Laut einer Studie von PwC haben Unternehmen nur in wenigen Fällen die Rolle eines Chief Process Officer (CPO) etabliert (11 %) oder eine ähnliche Funktion, die für die gesamte Prozesslandschaft verantwortlich ist. Dies wird als kritisch beurteilt, "da somit keine der Geschäftsführung oder dem Vorstand nahe Position im Unternehmen existiert, die Unternehmensziele auf Ebene der Prozessstrategie verfolgt und innerhalb des Geschäftsprozessmanagements umsetzt. Eine Person in solcher Funktion muss unter Umständen in der Lage sein, die Interessen des Geschäftsprozessmanagements ausgewogen und dennoch durchschlagskräftig vertreten zu können, wenn es zu Konflikten zwischen Ressorts und beteiligten Abteilungen kommt. Gerade die enge Verzahnung mit der IT-Abteilung verlangt einen CPO oder eine vergleichbare Position, die auf Augenhöhe mit dem Chief Information Officer (CIO) verhandeln kann." (PwC, 2011, S.29)

Auch die Interviewpartner haben teilweise auf die gute Erfahrung mit einer für das Prozessmanagement verantwortlichen Person berichtet und es als Voraussetzung für das effiziente GPM im Unternehmen angesehen. Es sollte immer jemand im Projekt involviert sein, der bereits Erfahrungen und Routine mit dem Prozessmanagement hat.

Prozessverantwortliche

Wie auch schon in der Beschreibung des Vorgehensmodells (in Kapitel 4.3) vorgestellt, wird empfohlen verschiedene Rollen einzuführen und zu besetzen. Nach Ansicht der Autorin und einiger Interview-Partner ist eine wichtige Voraussetzung für das GRC-GPM die Einführung eines Prozessverantwortlichen. Dieser muss für die Integration von GRC sensibilisiert und geschult sein und sich verantwortlich fühlen.

Versagt die Integration von verschiedenen Management-Disziplinen, so kann dies menschliche Gründe haben oder es gibt strukturelle Ursachen für das Silodenken. Unabhängig von der Ursache, kann dem Problem mit einer übergreifenden Verantwortung für Prozessrisiken begegnet werden.

Einige Interview-Partner gaben an, bereits Prozessverantwortliche implementiert zu haben. Diese sind die Abteilungsleiter der Abteilungen, in der die hauptsächliche Wertschöpfung des Prozesses stattfindet.

Kontinuierliche Verbesserung

Damit das GRC-GPM-System dauerhaft funktionieren kann, ist es wichtig dies kontinuierlich zu verbessern. Die Verbesserung kann nur erfolgen, wenn die Ergebnisse einer entsprechende Überwachung und Messergebnisse in die Verbesserung einfließen können.

So hat auch PwC (2011, S. 11) festgestellt: "Durch das Management von Geschäftsprozessen anhand von PLI kann die gesamte Prozesslandschaft des Unternehmens kontrolliert und analysiert werden. Diese Prüfung liefert die Basis für einen kontinuierlichen Verbesserungsprozess. Der Schlüssel liegt in der Ausgestaltung der PLI und in der Festlegung von Zielwerten, die durch ein branchenbezogenes oder branchenübergreifendes Benchmarking validiert werden. Durch dieses Vorgehen können Unternehmen Erfolge in der Verbesserung ihrer Prozesse transparent machen und objektiv vergleichen."

Prozessdokumentation

Es muss bei der Dokumentation von Prozessen und deren Visualisierung darauf geachtet werden, dass dies einheitlich geschieht. Für die Transparenz der Prozesse ist es nicht förderlich, wenn prozessuale Regelungen mal als Matrix, mal als Fließtext und mal als grafische Ablaufdarstellung umgesetzt werden. Der Vorteil für GRC, dass Risiken und Regelungen im Prozess dargestellt werden und die Umsetzung leichter geprüft werden kann ist dahin, wenn die Darstellung nicht einheitlich und für alle Beteiligten gleichermaßen zugänglich vorgenommen wird.

Dazu sollte es eine einheitliche Ablage geben und jemanden, der dafür zuständig ist. Außerdem sollte eine gemeinsame Notation festgelegt werden, mit der bestimmt wird, welche Diagrammtypen, Sichten, Symbole oder Namenskonventionen für die jeweiligen Prozessebenen, –sichten und -typen im Unternehmen zu nutzen sind.

Dann kann sich auch der Prüfer ganz auf den Inhalt konzentrieren und wir nicht durch unterschiedliche Darstellungen behindert und von möglichen Risiken abgelenkt.

Technologie

Software Technologie ist ein großes Thema im Rahmen der GRC-Untersuchungen. Die meisten Publikationen zum Thema GRC kommen von Softwarefirmen und Beratungshäusern, die diese Software einführen. Da ist es kaum verwunderlich, dass auch in den meisten Publikationen dazu hauptsächlich die passende technische Umsetzung beschrieben wird. Dies unterstreicht aber auch die Wichtigkeit der Technik als Unterstützung für das GRC-Management (Racz, Weippl und Seufert, 2010). Nach Ansicht der Autorin gilt dies auch für das integrierte GRC-GPM. Die entsprechende Technik kann die Integration und das Zusammengreifen der einzelnen Disziplinen unterstützen und zu großer Effizienz führen. Daher sollte bei der Einführung auch über die begleitende und unterstützende Technik nachgedacht werden.

Dabei muss jede Organisation entscheiden, ob sie eine Komplettlösung wählt, die sowohl die GRC-Funktionalitäten als auch die Prozessmodellierung in einer Anwendung integrieren, oder Einzellösungen. Bei den spezialisierten Anwendungen können die einzelnen Funktionsbereichen leistungsfähig sein, da diese bei einer Komplettlösung möglicher weise nur "abgespeckt" umgesetzt werden. Allerdings muss es dann Schnittstellen zwischen den Einzelanwendungen geben und bestenfalls eine gemeinsame Datenbank, um Felder für Risiken und Kontrollen integriert nutzen zu können.

Die Arbeit der Prüfinstanzen wird unterstützt, indem die Risiken und Kontrollen aus Prozessen leicht in eine Risiko-Kontroll-Matrix überführt werden können. So können dann Lücken durch fehlende Kontrollen für bestimmte Risiken ermittelt werden und mögliche mehrfache Kontrollen zum gleichen Risiko aufgespürt werden.

Umgekehrt ist ein integriertes IT-System auch für die Prozessmanager von Vorteil, da sie bei der Prozessmodellierung die bereits vorhandenen Risiken und Kontrollen sowie alle weiteren Datenbankfelder des Risikomanagementsystems (z.B. Risikoklassen, “Scoring” der Risiken, Verantwortliche für die Kontrollmaßnahmen) verwenden können.

6.2 Schwierigkeiten und Grenzen

Es gibt nur wenige wissenschaftliche Untersuchungen und Grundlagen zur integrierten Behandlung des GRC-Managements. GRC wird hauptsächlich aus der Wirtschaft heraus vorangetrieben und zu diesem Thema publizieren hauptsächlich Softwarefirmen, Analysten und Beratungshäuser. Die Grundlage in dieser Arbeit zum GRC-Management ist der

aktuelle Stand der Wissenschaft und die entsprechenden Einschränkungen gelten auch hier (Racz, Weippl und Seufert, 2010).

Damit das GRC-GPM System optimal eingesetzt werden kann, bedarf es einer kontinuierlichen Verbesserung. Als Grundlage dafür sind entsprechende Auswertungen notwendig. Diese erhält man aber nur, wenn bei einer systematischen Dokumentation aller Prozesse und der Erhebung von Kennzahlen. Es besteht die Gefahr, dass Prozesse in einigen Unternehmen nicht ausreichend analysiert und dokumentiert wurden. Diese Vermutung bekräftigt das Ergebnis einer PwC-Studie (2011): "Anhand unserer Umfrageergebnisse erkennen wir, dass sich Unternehmen gerade in einer Übergangsphase zwischen der Definition einzelner ausgewählter Geschäftsprozesse hin zu einer systematischen Dokumentation (Prozessmodellierung) aller relevanten Prozesse befinden. Kennzahlen und Berichte zu den Prozessen werden nur sporadisch (d. h. nur bei Bedarf) erhoben und ausgewertet."

Der Einsatz des Vorgehensmodells zur integrierten Einführung von GRC-Management und Prozessmanagement führt immer zu Veränderungen in der Organisation und am Arbeitsplatz der einzelnen Mitarbeiter. Es ist teilweise schwer nicht selbst initiierte Veränderungen anzunehmen. Das Projekt kann also am Widerstand und Boykott der Mitarbeiter scheitern. Es bedarf der konsequenten und sichtbaren Unterstützung durch die Unternehmensleitung und dem Einsatz von Change Management Aktivitäten, um diesen Schwierigkeiten entgegenzuwirken.

Solch umfänglichen Modelle, wie der GRC-GPM Ansatz, laufen schnell Gefahr, durch ihre Komplexität nicht realisierbar zu werden. Es werden hohe Kapazitäten an Zeit und Budget notwendig, um verschiedene Management Ansätze gleichzeitig im Unternehmen umzusetzen. Bei bestimmten Voraussetzungen ist es eventuell praktikabler schrittweise nacheinander und nicht integriert vorzugehen. Das bedeutet die Vorteile der Synergieeffekte würden bei der Einführung verloren gehen, dafür wäre der Projektumfang zu Anfang geringer. Nach Meinung der Autorin, sollte aber dann auch bei der nacheinander erfolgenden Einführung auf eine enge Verzahnung geachtet werden, um die beschriebenen Vorteile der Integration im Endergebnis zu erhalten. Zudem sollte auch immer der Aufwand für Prozessprojekte im Auge behalten werden. So geben Dräger und Rößler (2012, S.98) für ein durchschnittliches Projekt in einem mittelständigen Unternehmen einen Aufwand von bis zu 50 Manntagen an (für das GPM nach NOVACESS). Werden die GRC-Faktoren erste nachträglich in einem zweiten Projekt in die Prozesse integriert, so kann sich dieser Aufwand verdoppeln.

Frigo und Anderson (2009) empfehlen einen einfachen und schlanken Ansatz: „Furthermore, internal auditors can help stakeholders understand that with the relative newness of GRC, a simple, iterative approach should be used to implement the initiative, giving all GRC functions opportunities to understand fully the objectives and goals.“ Allerding überwiegen nach Meinung der Autorin die Vorteile des integrativen Vorgehens und mit einem effektiven Change Management sollte diesen Bedenken begegnet werden können.

Das vorgestellte Modell stößt auch dann an seine Grenzen, wenn Zielkonflikte zwischen GRC -Management und GPM vorliegen. Das Geschäftsprozessmanagement zielt auf möglichst flexible und agile Geschäftsprozesse ab. Das GRC-Management auf der anderen Seite strebt nach möglichst effektiven Regeln, Kontrollen und daraus resultierenden Prozessvorgaben. Dies kann nach Ansicht der Autorin in den Augen von Verantwortlichen zu einem Zielkonflikt führen. Ein möglichst schlanker und flexibler Prozess möchte in dieser Sichtweise auf jegliche Kontrollschleife und Risikoprävention verzichten. Um diesem Problem zu begegnen, ist es wichtig das große Ganze zu betrachten und immer bereits beschriebenen Nachteile und Risiken vor Augen zu führen, die mit einer Vernachlässigung der GRC-Disziplinen einhergehen.

Eine weitere Schwierigkeit, nach Ansicht der Interview-Partner, ist die Zusammenarbeit von Fachabteilungen/ Personen, die vor der Einführung von GRC-GPM getrennt voneinander gearbeitet haben. Es ist mit Widerstand zu rechnen, wenn neue Strukturen eingeführt werden. Für den Projektverlauf müssen die Kernkompetenzen der GRC-Disziplinen und des Prozessmanagements zusammenkommen, was bedeuten kann, dass sehr große Projektteams entstehen. Dies kann dazu führen, dass Entscheidungen sehr lange dauern und es entsteht Konfliktpotenzial. Die betriebswirtschaftliche Sicht der einen kann mit der Compliance- und Risikosicht der anderen kollidieren. Daher sollte bei der Teamauswahl sehr genau darauf geachtet werden, wer ausgewählt wird. Es sollte ein fähiger und effizienter Projektleiter gewählt werden und über entsprechende Team-Building Maßnahmen nachgedacht werden.

7 Fazit und Ausblick

Wissenschaft und Gesellschaft konzentrieren sich häufig nur auf einzelne Problemstellungen und Themen und beschäftigen sich mit diesen meist nur getrennt voneinander. So sind z.B. diverse ISO-Normen in Unternehmen weit verbreitet, die verschiedene Gebiete, wie Qualitätsmanagement, Risikomanagement und Compliance-Management isoliert voneinander betrachten. Diese Themen werden dann erst recht nicht im Zusammenhang mit dem Prozessmanagement analysiert und implementiert.

In dieser Arbeit wurden die Vorteile und Synergieeffekte einer integrierten Vorgehensweise dargestellt. Dabei hat sich die Autorin auf die Integration von GRC-Management und Geschäftsprozessmanagement konzentriert und ein integriertes Vorgehen zur Einführung und Implementation im Unternehmen vorgestellt. Die Integration kann und sollte nach Ansicht der Autorin aber noch über dieses Modell hinaus weiter gehen. Das Prozessmanagement sollte gleichzeitig mit weiteren Management-Disziplinen wie Wissensmanagement oder Qualitätsmanagement eng verzahnt werden. Hier sieht die Autorin weiteren Forschungbedarf.

Am GRC-Management führt kein Weg vorbei. Auf Grund von diversen gesetzlichen Regelungen müssen Unternehmen in Risikomanagement, Governance und Compliance-Management-Systeme investieren. Trotzdem gibt es noch Defizite in der wissenschaftlichen Forschung zum Thema GRC-Management. Die Informationen zu dem Thema bleiben eher Abstrakt. Die Autorin sieht weiterführenden Bedarf an wissenschaftlichen Untersuchungen zum Thema GRC-Management, damit auf dieser Basis ein noch ausführlicheres integriertes Modell und eine noch effektivere Fusion mit dem Prozessmanagement geschaffen werden kann.

Der integrierte Ansatz hat sowohl auf das Geschäftsprozessmanagement positive Auswirkungen, also auch auf das GRC-Management. Prozessmanagement und GRC bilden ein optimales Gespann: wer Abläufe beschreibt, mit Regeln, Risiken und Unternehmenszielen- und werten verknüpft und das Ergebnis über eine eingängige Visualisierung an das gesamte Unternehmen kommuniziert, der schafft die besten Voraussetzungen dafür, dass Regeln bekannt sind und eingehalten werden, Risiken effektiv gesteuert werden und Unternehmensziele und -werte umgesetzt werden.

Literatur

Bayer und Kühn, 2013	Bayer, Franz; Kühn, Harald: Prozessmanagement für Experten. - 1. Aufl. Berlin Heidelberg: Springer-Verlag 2013
Becker, Kugeler und Rosemann, 2012	Becker, Jörg; Kugeler, Martin; Rosemann, Michael: Prozessmanagement. - 7. Aufl. Berlin, Springer-Verlag, 2012
BPTrends BPM, 2012	The State of Business Process Management http://www.bptrends.com/bpt/wp-content/surveys/2012-_BPT%20SURVEY-3-12-12-CW-PH.pdf verfügbar am 01.12.2015, 09:16 Uhr
BPTrends Process Centers, 2012	Business Process Centers of Excellence Survey http://www.bptrends.com/bpt/wp-content/surveys/2012-BPTrends-CoE-Survey-3.pdf verfügbar am 01.12.2015, 09:10 Uhr
DCGK, 2015	www.dcgk.de/de/ verfügbar am 04.11.2015, 14:13 Uhr
Deloitte, 2008	Growing confidence (the smart way to manage governance, risk, and compliance). http://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/Corporate%20Governance/Audit%20Committee/in-gc-growing-confidence-a-smart-way-to-manage-governance-risk-and-compliance-noexp.pdf verfügbar am 28.10.2015, 09:25 Uhr
DFG, Leopoldina 2014	http://www.dfg.de/download/pdf/dfg_im_profil/reden_stellungnahmen/2014/dfg-leopoldina_forschungsrisiken_de_en.pdf verfügbar am 23.10.2015, 10:13 Uhr

Dillerup und Stoi, 2011 — Dillerup, Ralf; Stoi, Roman: Unternehmensführung. - 3. Aufl. München, Verlag Franz Vahlen, 2011

Dräger und Rößler, 2012 — Dräger, Erich; Rößler, Steffen: Prozessmanagement. - 1. Auflg. Röthenbach: Resultance GmbH Eigenverlag, 2012

Fischermanns, 2014 — Fischermanns, Prof. Dr. Guido: Prozessfenster-blog http://prozessfenster-blog.de/2014/03/04/chancen-der-integration-von-iks-risikomangement-compliance-und-prozessmanagement/ verfügbar am 14.11.2015, 12:01 Uhr

Frigo und Anderson, 2009 — Frigo, Mark; Anderson, Richard: Strategic GRC: 10 Steps to Implementation
In: Internal Auditor (2009), Nr. 66, S. 33-37. - ISSN 0020-5745

Gabler, 2015 — Fiege, Prof. Dr. Stefanie: Gabler Wirtschaftslexikon. http://wirtschaftslexikon.gabler.de/Definition/risikomanagement.html#definition
verfügbar am 22.11.2015, 17:38 Uhr

Holz, 2015 — Holz, Alexander: Compliance-relevante Reformvorschläge im Vergleich
In: Comply (2015), Nr. 1, S. 12-13. - ISSN 2364 - 7604

IDW PS, 2011 — IDW Prüfungsstandard: Grundsätze ordnungsmäßiger Prüfung von Compliance Management Systemen. - 1. Auflg. Düsseldorf, IDW Verlag, 2011

Junker, 2014 — Junker, Manuel: Prozessmanagement - Abriss der Geschichte; http://www.organisationshandbuch.de/organisationshandbuch-prozessmanagement/allgemeine-informationen-prozessmanagement/prozessmanagement-abriss-der-geschichte/, verfügbar am 25.07.2014, 09:23 Uhr

Kochanowski et. al, 2014 — Kochanowski, Monika; Drawehn, Jens; Kötter, Falko; Renner, Thomas: Compliance in Geschäftsprozessen. - 1. Aufl. Stuttgart, Fraunhofer Verlag, 2014

Krems, 2012 — Krems, Dr. Burkhardt: Online-Verwaltungslexikon http://www.olev.de/c/corporate_governance.htm verfügbar am 17.11.2015, 12:33 Uhr

Krügler, 2011 — Krügler, Eberhard: Compliance - ein Thema mit vielen Facetten. In: Umwelt Magazin (2011), Nr 7/8, S. 50

Marekfia und Nissen, 2009 — Marekfia, Wolfgang; Nissen, Volker: Strategisches GRC-Management - Grundzüge eines konzeptionellen Bezugsrahmens. In: Forschungsberichte zur Unternehmensberatung (2009), Nr. 2. - ISSN 1862-1805

Menzies, 2009 — Menzies, Christof: Sarbanes-Oxley und Corporate Compliance - Nachhaltigkeit, Optimierung, Integration. - 1. Auflg. Stuttgart, Schäffer-Poeschel, 2009

NOVACESS, 2015 — http://www.novacess.de/best-practice/vorgehensmodell-prozessprojekt/ verfügbar am 05.11.2015, 11:07 Uhr

NTT DATA, 2013 — http://emea.nttdata.com/de/aktuelles/news-detailansicht//article/ntt-data-studie-zeigt-handlungsbedarf-beim-compliance-management/index.html verfügbar am 29.10.2015, 10:15 Uhr

OECD, 2004 — OECD-Grundsätze der Corporate Governance http://www.oecd.org/corporate/ca/corporategovernanceprinciples/32159487.pdf verfügbar am 17.11.2015, 12:24 Uhr

PMI, 2015 www.pmi.org
verfügbar am 05.11.2015, 14:35 Uhr

PwC, 2004 PwC, White Paper: Integrity-Driven Performance
http://www.grc-resource.com/resources/pwc_integritydrivenperformance.pdf
verfügbar am 29.11.2015, 9:22 Uhr

PwC, 2005 PricewaterhouseCoopers: 8th annual global CEO survey
http://www.globes.co.il/Serve/Researches/documents/8thannualglobalceosurvey.pdf
verfügbar am 01.11.2015, 16:31 Uhr

PwC, 2011 PricewaterhouseCoopers: Zukunftsthema Geschäftsprozessmanagement
https://www.pwc.de/de/prozessoptimierung/assets/pwc-gpm-studie.pdf
verfügbar am 05.11.2015, 9:45 Uhr

Racz, Weippl und Seufert, 2010 Racz, Nicolas; Weippl, Edgar; Seufert, Andreas: (2010): A frame of reference for research of integrated GRC.
In: Communications and Multimedia Security 11th IFIP TC 6/TC 11 International Conference (2010), S. 106-117. - ISBN 978-3-642-13240-7

Rieke und Winkelmann, 2008 Rieke, Dr. Tobias; Winkelmann, Dr. Axel: Modellierung und Management von Risiken - Ein prozessorientierter Risikomanagement-Ansatz zur Identifikation und Behandlung von Risiken in Geschäftsprozessen
In: Wirtschaftsinformatik (2008), Nr. 5, S. 346-356. - ISSN 0937-6429

Riemann, 2012 Riemann, Ute: Compliance im Prozessmanagement.
In: ERP Management (2012), Nr. 8, S.33-35. - ISSN 1860-6725

Romeike, 2008 — Romeike, Frank: Rechtliche Grundlagen des Risikomanagements. - 1. Aufl. Berlin, Erich Schmidt Verlag, 2008

Sadiq, Governatori und Naimiri, 2007 — Sadiq, Shazia; Governatori, Gido; Naimiri, Kioumars: Modeling Control Objectives for Business Process Compliance
In: 5th International Conference BPM (2007), Nr. 5 S. 149-164. - ISBN 978-3-540-75182-3

Schmelzer und Sesselmann, 2013 — Schmelzer, Hermann; Sesselmann, Wolfgang: Geschäftsprozess-Management in der Praxis. - 8. Aufl. München: Carl Hanser Verlag, 2013

Schmidt, 2009 — Schmidt, Prof. Dr. Werner: Integrierter Business-Process-Management-Zyklus
In: Arbeitsberichte – Working Papers (2009), Nr. 16 S. 1 - 32. - ISSN 1612-6483

Schnetzer, 2014 — Schnetzer, Ronald: Achtsames Prozessmanagment. - 1.Aufl. Wiesbaden: Springer Gabler 2014

Schweikert, 2014 — Schweikert, Christine: Generische Compliance-Risiken in mittelständischen und Großunternehmen – Auswertung vorliegender Studien zu Compliance, Integrity und Wirtschaftskriminalität.
In: KICG - Forschungspapiere (2014), Nr. 8. - ISSN 2198-4913

Streck und Binnewies, 2009 — Streck, Dr. Michael; Binnewies, Dr. Burkhard: Tax Compliance
In: DStR Deutsches Steuerrecht (2009), Nr. 5, S. 185-248. - ISSN 0949-7676

Wecker und van Laak, 2009 — Wecker, Dr. Gregor; van Laak, Hendrik: Compliance in der Unternehmerpraxis. - 2. Auflg. Wiesbaden, Gabler, 2009

Weilkiens, — Weilkiens, Tim; Weiss, Christian; Grass, Andrea: Basiswissen

Weiss und Grass, 2010 — Geschäftsprozessmanagement. - 1. Aufl. Heidelberg, dpunkt.verlag, 2010

Weuster, 2014 — Weuster, Sandra: Werkzeugunterstützung fü Governance, Risk und Compliance Management. https://www.softwareforen.de/portal/media/softwareforenleipzig/wissen/eigene_publikationen/Werkzeugunterstuetzung_fuer_Governance_Risk_und_Compliance_Management_-_Anwendungen_und_Marktuebersicht.pdf verfügbar am 29.10.2015, 14:01 Uhr

Wieland et. al, 2010 — Wieland, Josef; Steinmeyer, Roland; Grüninger, Stephan: Handbuch Compliance - Management. - 1. Aufl. Berlin: Erich Schmidt Verlag, 2010

Wieland, 2008 — Wieland, Josef: Die Kunst der Compliance In: Wirtschaftskriminalität und Ethik (2008), Nr. 16, S. 155-169. - ISBN 978-3-86618-234-9

zur Muehlen und Ho, 2006 — zur Muehlen, Michael; Ho, Danny Ting-Yi: Risk Management in the BPM Lifecycle.. In: Business Process Managements Workshops (2006), S. 454-466. - ISBN 978-3-540-32596-3

Anlagen

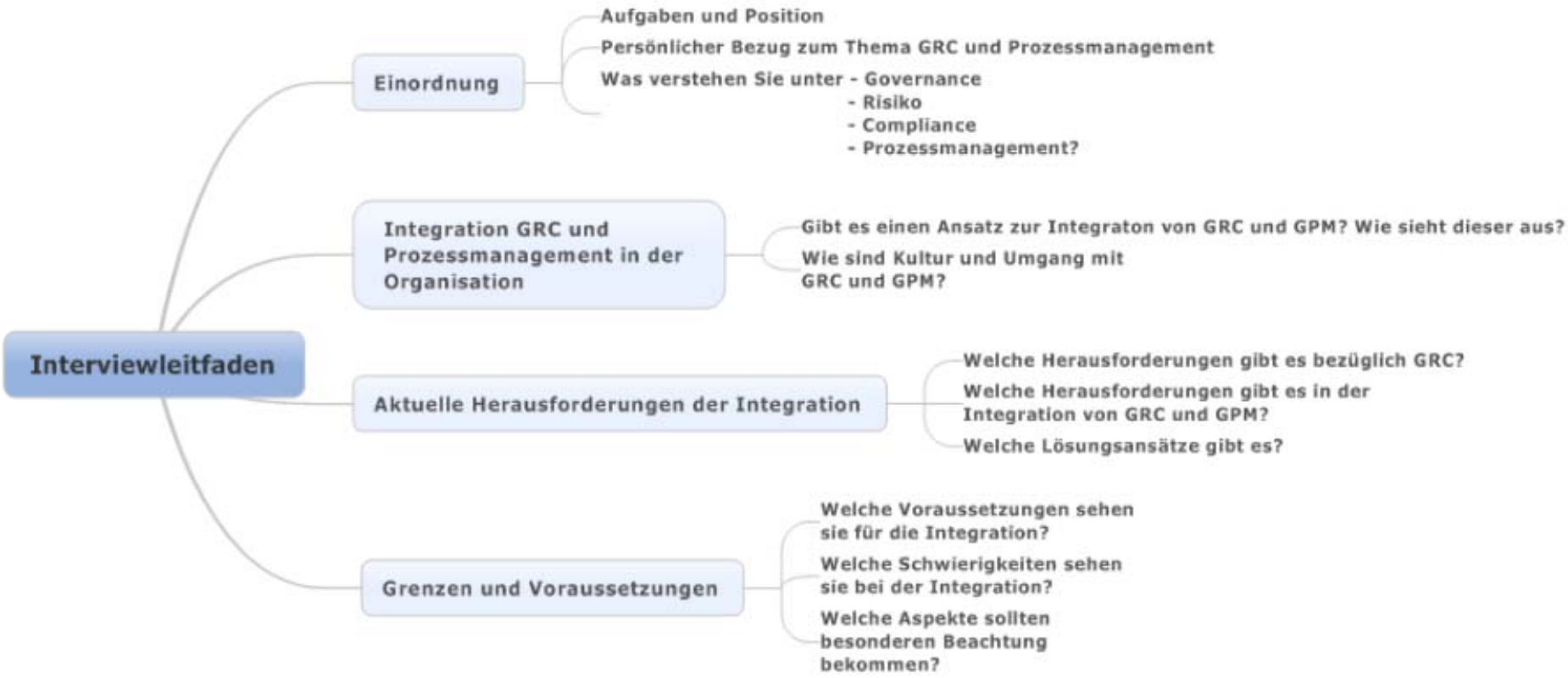
Anlage

Interview zur Integration von GRC und GPM

Die Interviews wurden in Form von qualitativen leitfragengestützten Interview-Fragen mit einer offenen Fragestellung geführt.

Befragt wurden Mitarbeiter aus verschiedenen Forschungsgesellschaften (Fraunhofer-Gesellschaft, Max-Planck-Gesellschaft, Helmholtz-Gemeinschaft, KIT), deren Arbeits-schwerpunkte in den Themen-Bereichen Prozessmanagement, Compliance, Governance und/ oder Risikomanagement liegen. Die Organisationen der befragten Interview-Partner sind in unterschiedlichen Stadien der Umsetzung von GRC und von Prozessmanagement. Es sind funktional aufgebaute Organisationen. Die Ergebnisse der Interviews sind in den Kapiteln 5 und 6 wiedergegeben.

Die Punkte auf dem nachfolgenden Leitfaden haben als grobe Orientierung gedient.


Interviewleitfaden
Einordnung
Aufgaben und Position
Persönlicher Bezug zum Thema GRC und Prozessmanagement
Was verstehen Sie unter - Governance
- Risiko
- Compliance
- Prozessmanagement?
Integration GRC und Prozessmanagement in der Organisation
Gibt es einen Ansatz zur Integraton von GRC und GPM? Wie sieht dieser aus?
Wie sind Kultur und Umgang mit GRC und GPM?
Aktuelle Herausforderungen der Integration
Welche Herausforderungen gibt es bezüglich GRC?
Welche Herausforderungen gibt es in der Integration von GRC und GPM?
Welche Lösungsansätze gibt es?
Grenzen und Voraussetzungen
Welche Voraussetzungen sehen sie für die Integration?
Welche Schwierigkeiten sehen sie bei der Integration?
Welche Aspekte sollten besonderen Beachtung bekommen?

Selbstständigkeitserklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbstständig und nur unter Verwendung der angegebenen Literatur und Hilfsmittel angefertigt habe.

Stellen, die wörtlich oder sinngemäß aus Quellen entnommen wurden, sind als solche kenntlich gemacht.

Diese Arbeit wurde in gleicher oder ähnlicher Form noch keiner anderen Prüfungsbehörde vorgelegt.

München, den 13. Dezember 2015

Hanna Sintermann